pd2

1.A Factorisation in rings

In this section we extend the concepts of divisibili greatest common divisor, prime elements in the ring of integers $\mathbb{Z}$ to arbitrary rings and study those integral domains in which an analogue of the Fundamental Theorem of Arithmetic holds. This study is modeled on properties of the ring of integers.

Let A be a commutative ring with unity $1_A = 1$.

1.A.1 Definitions Let $a, b \in A$. We say that a divides b or b is divisible by a or b is a multiple of a or a is a factor of b if there exists an element $c \in A$ with $b = ca$ and is denoted by $a \mid b$.

Below we shall give several definitions and properties for reference.

(1) The divisibility $\mid$ is a relation on A, it is reflexive, i.e. $a \mid a$ for every $a \in A$ and transitive, i.e. for $a, b, c \in A$, if $a \mid b$ and $b \mid c$, then $a \mid c$. But it is not symmetric, for example, $1 \mid 2$ in $\mathbb{Z}$, but $2 \nmid 1$ in $\mathbb{Z}$.

(2) $1 \mid a$ and $a \mid 0$ for every $a \in A$. Moreover, 1 is the smallest element and 0 is the greatest element with respect to the divisibility relation.

(3) (Compatibility of divisibility with addition and multiplication) For $a, b, c, d \in A$, we have:

(i) if $a|b$ and $a|c$, then $a|\lambda b+\mu c$ for every $\lambda, \mu \in A$

(ii) if $a|b$ and $c|d$, then $ac|bd$, in particular, $ac|bc$

(iii) if c is a non-zero divisor in A and if $ac|bc$, then $a|b$.

(4) The units in A (invertible elements with respe to the multiplication in A) are characterized by:
$u \in A^{\times}$ (= the group of units in A) $\Longleftrightarrow$ $u|a$ for every a
$\Longleftrightarrow$ $u|1$.

(5) Two elements $a, b \in A$ are said to <u>associates</u> if $a|b$ and $b|a$. The relation "a is an associate of b" is an equivalence relation on A. The equivalence class of 1 is precisely the set of all units $A^{\times}$ and the equivalence class of 0 is the singleton $\{0\}$.

For $a, b, c \in A$, we have:

(i) Suppose that a and b are associates. Then $a|c$ if and only $b|c$.

(ii) If $b = ua$ for some unit $u \in A^{\times}$, then a and b are assocites.

(iii) If a is non-zero divisor in A, then b is an associate of a if and only if $b = ua$ for some uni $u \in A^{\times}$. In particular, associate of a non-zero divisor must be a non-zero divisor.

(6) A divisor a of b is called a <u>trivial</u> (or <u>improper</u>) <u>divisor</u> if either a is unit in A or a and b are associates; otherwise a is called a <u>proper divisor</u> of b and in this case we use the notation $a \| b$.
Units have no proper divisors; Every proper divisor of 0 is a non-unit.

Let $a, b, c \in A$ with $b = ac$. Suppose that b is a non-zero divisor in A. Then $a \| b \iff c \| b$.

1.A.2 Examples

(1) Let $a = 2$, $b = 3$, $c = 3$ in $\mathbb{Z}_6$. Then $ac = 4 | 0 = bc$ but $a \nmid b$.

(2) In $\mathbb{Z}$, the integers a and b are associates if and only if $a = \pm b$, i.e. $|a| = |b|$.

(3) Let $F := X(1 - YZ) \in \mathbb{Z}[X, Y, Z]$ and let $A := \mathbb{Z}[X, Y, Z]/(F) = \mathbb{Z}[x, y, z]$ be the quotient ring. Then the elements x and xy are associates, since $x = xyz$ in A, but $xy \neq ux$ for every $u \in A^\times$. Suppose that $U = \sum a_{ijk} X^i Y^j Z^k \in \mathbb{Z}[X, Y, Z]$ be such that $\overline{U} = u \in A^\times$ and $xy = ux$. Then, since $A/Ax = \mathbb{Z}[Y, Z]$ and $\overline{u} \in (A/Ax)^\times$, we must have $U = a + Xf$ with $a \in \mathbb{Z}$ and $f \in \mathbb{Z}[X, Y, Z]$. Now, from $xy = ux$ in A we have $UX - XY = X(1 - YZ)g$ for some $g \in \mathbb{Z}[X, Y, Z]$. Cancelling X on both sides and putting $U = a + Xf$ we get $a + Xf - Y = (1 - YZ)g$; again putting $X = 0$ we get that the polynomial $a + Y = (1 - YZ)g(0, Y, Z)$ has degree ≥ 2 a contradiction.

(4) In the polynomial ring $A[X]$ over an integral domain A the polynomials $f, g \in A[X]$ are associates if and only if $f = ug$ with $u \in A^\times$; this is clear from $A[X]^\times = A^\times$. Therefore an equivalence class of a non-zero polynomial with respect to the equivalence relation associates in $A[X]$ contains exactly one monic polynomial.

<u>**1.A.3 Definition**</u> An element $a \in A$ is called <u>irreducible</u> or <u>indecomposable</u> if it is a non-zero divisor, non-unit and if it has no decomposition $a = bc$ into non-units $b, c \in A$, otherwise we say that a is <u>reducible</u> or <u>decomposable</u>. Note that irreducible elements in A are non-zero divisors, (in particular $\neq 0$), non-units and has no proper divisors in A. Further, an associate of an irreducible element is irreducible.

<u>**1.A.4 Lemma**</u> Let $a \in A$ be a non-zero divisor, non-unit in A. Then a is irreducible in $A \iff a$ has no proper divisors in A.

<u>Proof</u> ($\Rightarrow$) Noted above. ($\Leftarrow$) If $a = bc$ with $b, c \in A$, then $b | a$ and hence either $b \in A^\times$ or b is an associate of a in A. (by assumption) In the second case $b = ua$ for some $u \in A^\times$ (since a is a non-zero divisor in A) and hence $1 = uc$, i.e c is a unit in A. Therefore $a = bc$ is not a proper decomposition.

<u>**1.A.5 Definition**</u>

An element $p \in A$ is called a <u>prime element</u> in A if it is a non-zero divisor and if the principal ideal Ap generated by p is a prime ideal in A or equivalently if the quotient ring A/Ap is an integral domain.
Note that prime elements in A are non-zero divisors (in particular $\neq 0$), non-units. Further an associate of a prime element is a prime element.

Prime elements can be characterized by divisibility:

1.A.6 Lemma For a non-zero divisor $a \in A$, the following statements are equivalent:

(i) a is a prime element.

(ii) a is not a unit in A and if $a \mid bc$ with $b, c \in A$, then either $a \mid b$ or $a \mid c$ in A.

1.A.7 Corollary If a prime element $p \in A$ divides a product $a_1 \cdots a_n$ of elements $a_1, \dots, a_n \in A$, then $p \mid a_i$ for some i with $1 \leq i \leq n$.

1.A.8 Corollary Every prime element in A is irreducible.

Proof Let $a \in A$ be a prime element. If $a = bc$ with $b, c \in A$, then by 1.A.6 either $a \mid b$ or $a \mid c$. Suppose that $a \mid b$ i.e. $b = ad$ with $d \in A$. Then $a = bc = adc$ and hence (Since a is a non-zero divisor in A) $1 = dc$, i.e. $c \in A^\times$. Therefore $a = bc$ is not a proper decomposition.

1.A.9 Examples

(1) In $A = \mathbb{Z}$ (or more generally in a PID see) the concepts of prime and irreducible are same and these are precisely $\pm p$, where p is a prime number.

(2) Let K be a field and let $A = K[X^2, X^3] = \{a_0 + a_2X^2 + a_3X^3 + \cdots + a_nX^n \mid a_0, a_2, \ldots, a_n \in K\} \subseteq K[X]$. Then X^2 and X^3 are irreducible in A (can be easily seen by comparing degrees), but they are not prime, since X^2 and X^3 divides $(X^3)^2 = X^6 = (X^2)^3$, but $X^2 \nmid X^3$ in A and $X^3 \nmid X^2$ in A.

(3) Prime elements in the polynomial ring $B = A[X_i]_{i}$ are called <u>prime polynomials</u>. If A is an integral domain the elements $bX_i - a$ with $a \in A$, $b \in A^\times$ are prime polynomials in B. In particular, if $A = K$ is a field, then every polynomial of degree 1 in B is a prime polynomial in B. ($B/(bX_i - a) \cong A[X_j \mid j \in I, j \neq i]$ is an integral domain and $0 \neq bX_i - a \notin B^\times = A^\times$).

(4) Let $a \in A$ be a non-zero divisor and a non-unit in A. Then a is a prime element in $A \iff a \in A[X]$ is a prime element in $A[X]$ ($A[X]/aA[X] \cong A/(a)[X]$

(5) Let $f \in A[X]$ be a monic polynomial over an integral domain. Suppose that $1 \leq \deg f \leq 3$. Then f is an irreducible element in $A[X]$ if and only f has no zero in A. ($\Leftarrow$: Since f is monic and $\deg f \geq 1$, $f \notin A[X]^\times = A^\times$ and non-units in A are not divisors of f. Therefore, if f is reducible in $A[X]$, then

by degree formula $f = (aX+b)h$ for some $a, b \in A$ further $a \in A^\times$, since f is monic. Then $-b/a \in A$ is a zero of f in A.

(Remark If $a \in A$ is a zero of a non-constant polynomial $f \in A[X]$, i.e. $f = (X-a)h$ with $h \in A[X]$, then $f(0) = -a\,h(0)$ and hence a is a divisor of $f(0)$ in A). For example, the polynomial $f = X^3 + 2X^2 + X + 4 \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Z}$, since divisors of 4 are not zeros of f.

(5) In the polynomial ring $\mathbb{C}[X]$ over the field of complex numbers, the prime polynomials are precisely the polynomials of degree 1 (this is precisely the Fundamental Theorem of Algebra). In $\mathbb{R}[X]$ prime polynomials are precisely polynomials of degree 1 and quadratic polynomials $X^2 + aX + b$, $a, b \in \mathbb{R}$ with negative discriminants i.e. $a^2 - 4b < 0$. (This follows from intermidiate value theorem and fundamental theorem of algebra). The description of prime polynomials in $\mathbb{Q}[X]$ or in $K[X]$ where K is a finite field is more complex.

For a prime number $p \in \mathbb{N}$, the polynomial $X^2 - p \in \mathbb{Z}[X]$ is an irreducible polynomial –

(7) In the ring $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$, wher m is a squaree free integer, the element 2 is not prime. Since $2 \mid m(m-1) = (m+\sqrt{m})(m-\sqrt{m})$, but $2 \nmid m+\sqrt{m}$ and $2 \nmid m-\sqrt{m}$ in $\mathbb{Z}[\sqrt{m}]$.

(8) Let $m \in \mathbb{Z}$ be a square free integer with $m \leq -3$. Then the element 2 is irreducible in $\mathbb{Z}[\sqrt{m}]$.

Suppose that $a+b\sqrt{m}$, $c+d\sqrt{m}$ are non-units in $\mathbb{Z}[\sqrt{m}]$ with $2 = (a+b\sqrt{m})(c+d\sqrt{m})$. Then $4 = N(2) = N(a+b\sqrt{m})\,N(c+d\sqrt{m})$ and hence (by the fundamental theorem arithmetic) $|N(a+b\sqrt{m})| = |N(c+d\sqrt{m})| = 2$, since both $a+b\sqrt{m}$ and $c+d\sqrt{m}$ are non-units. But $N(a+b\sqrt{m})) = a^2 - b^2 m = \begin{cases} \geq (-m)b^2 \geq 3 > \pm 2, & \text{if } b \\ a^2 \neq \pm 2, & \text{if } b = \end{cases}$

a contradiction. This proves that 2 is irreducible in $\mathbb{Z}[\sqrt{m}$

(9)

Divisibility properties in a ring can also be described by using (principal) ideals.

1.A.10 Let $a, b \in A$. Then:

(1) $a \mid b \iff Ab \subseteq Aa$

(2) a and b are associates in $A \iff Ab = Aa$.

(3) $a \in A^{\times} \iff Aa = A$.

(4) $a \parallel b \iff Ab \subsetneq Aa \subsetneq A$.

(5) a is an irreducible element in $A \iff$ the principal ideal Aa is maximal (with respect to the inclusion in the family of proper principal ideals in A.

Proof

1.A.11 Definitions A sequence $a_n, n \in \mathbb{N}$ of elements in A is called a chain of divisors if a_{n+1} divides a_n for every $n \in \mathbb{N}$.

We say that a ring A satisfies divisibility chain condition if every chain of divisors $a_n, n \in \mathbb{N}$ in A is stationary, i.e. $\exists\, n_0 \in \mathbb{N}$ such that a_{n+1} and a_n are associates in A for every $n \geq n_0$, i.e. $Aa_{n+1} = Aa_n$ for every $n \in \mathbb{N}, n \geq n_0$.

Note that a ring A satisfies divisibility chain condit on if and only if every ascending chain of principal ideals in A is stationary. In particular, every noetherian ring satisfies divisibility chain condition.

1.A.12 Theorem Let A be a ring which satisfies the divisibility chain condition. Then every non-zero element $a \in A$ is a product of irreducible elements.

Proof Suppose that $a \neq 0$ is not a product of irreducible elements in A, in particular, a is not irreducible in A, i.e. $a = a_1 b_1$ with $a_1, b_1 \in A \setminus (A^\times \cup \{0\})$, i.e. $a_1 || a$, $b_1 || a$. If both a_1 and b_1 are product of irreducible elements in A, then $\overset{a_0=}{a} = a_1 b_1$ is also a product of irreducible elements in A. We may assume that a_1 is not a product of irreducible elements in A. Then $a_1 = a_2 b_2$ with $a_2, b_2 \in A \setminus (A^\times \cup \{0\})$. Continuing the above process, we construct a sequence $a_n, n \in \mathbb{N}$ such that $a_{n+1} || a_n$ for every $n \in \mathbb{N}$, i.e. the sequence $a_n, n \in \mathbb{N}$ is a chain of proper divisors and hence is not sationary

<u>**1.A.13 Theorem**</u> Let $p_1, \dots, p_m, q_1, \dots, q_n \in A$ be prime elements and let $a := p_1 \cdots p_m$, $b := q_1 \cdots q_n$. Then:

(1) If $a|b$, then $m \le n$.

(2) If $a||b$, then $m < n$.

(3) If $a = b$, then $m = n$ and there exists a permutation $\sigma \in \mathfrak{S}_n$ such that p_i and $q_{\sigma(i)}$ are associates for every $i = 1, \dots, m$.

<u>Proof</u>

1.A.14 Definition A ring A is called factorial or unique factorisation domain if it is an integral domain and every non-zero, non-unit is a product of prime elements.

For example the ring of integers $\mathbb{Z}$ is factorial (this is precisely the fundamental theorem of arithmeti

In a factorial ring A every irreducible element a is prime, since in a product representation of a into prime elements only one prime can occur. Therefore:

1.A.15 Lemma Let A be an integral domain. The A is factorial if and only if:

(1) Every non-zero, non-unit is a product of irreduci elements.

(2) Every irreducible element is prime.

In particular, in factorial rings irreducible elements and prime elements are identical

Note that for a given integral domain verifying the condition (2) of 1.A.15 is more difficult than verifying the condition (1) of 1.A.15 (see 1.A.12).

Let A be a factorial domain and let $\mathbb{P}$ be a comple representative set for the equivalences classes of prir elements under the equivalence relation "being an associate of". For example if $A=\mathbb{Z}$, then the set $\mathbb{P}=\{p\in\mathbb{N} \mid p \text{ prime number}\}$ is a complete representati

set for the equivalence classes of prime elements in $\mathbb{Z}$
By definition of factoriality and 1.A.13, every non-zero $a \in A$ can be written uniquely in the form:

$$a = e \prod_{p \in P} p^{v_p(a)}$$

Where $v_p(a) \in \mathbb{N}$ for every $p \in P$ and $v_p(a) = 0$ for almo all $p \in P$ and e is (uniquely determined by a) a unit in
We put $v_p(0) = \infty$ for every $p \in P$.
For $p \in P$ and $0 \neq a \in A$, the natural number $v_p(a)$ is called the <u>p-th exponent</u> of $a \in A$.
Let K be the quotient field of A. For $p \in P$ and $0 \neq x = a/b \in K$, $a, b \in A$, $b \neq 0$, we put $v_p(x) = v_p(a) - v_p(b)$ (this is well-defined: if $a/b = a'/b'$, then $ab' = a'b$ and so $v_p(a) + v_p(b') = v_p(ab') = v_p(a'b) = v_p(a') + v_p(b)$). Therefore:

$$x = e \prod_{p \in P} p^{v_p(x)}$$

Where $v_p(x) \in \mathbb{Z}$ for every $p \in P$ and $v_p(x) = 0$ for all m all $p \in P$ and e is (uniquely determined by x) a unit in
Therefore we get the representation: $x = e\frac{c}{d}$, where $c = \prod_{v_p(x) \geq} p$
and $d := \prod_{v_p(x)<0} p^{-v_p(x)}$ and are called <u>numerator</u> and <u>denominator</u>.

<u>**1.A.15 Properties of the p-exponents**</u> Let A be a factorial domain and let $x, y \in K = q^t$ field of A.
Then:

(1) If $x \neq 0$, then $v_p(x) = 0$ for all most all $p \in P$.

(2) $v_p(xy) = v_p(x) + v_p(y)$ for every $p \in P$.

(3) $v_p(x+y) \geq \operatorname{Min}\{v_p(x), v_p(y)\}$ for every $p \in P$.

(4) $v_p(x) = 0$ for every $p \in P$ if and only if $x \in A^\times$

(5) $v_p(x) \leq v_p(y)$ for all $p \in P$ if and only if there exists $a \in A$ with $xa = y$, i.e. $x | y$ in A.

(6) $v_p(x) = v_p(y)$ for all $p \in P$ if and only if there exists $e \in A^\times$ with $xe = y$, i.e. x and y are associates in A

(7) $v_p(x) \geq 0$ for all $p \in P$ if and only if $x \in A$.

<u>Proof</u> Exercise.

1.A.16 Definition Let $a, b \in A$. An element $d \in A$ is called a greatest common divisor of a and b in A if

(1) $d|a$ and $d|b$

(2) if $t \in A$ and $t|a$, $t|b$, then $t|d$.

An element $m \in A$ is called a least common multip of a and b in A if

(1) $a|m$ and $b|m$

(2) if $e \in A$ and $a|e$, $b|e$, then $m|e$.

Note that any two gcds (and lcms) of a and b are associates. Therefore in an integral domain the gcd (resp. lcm) of $a, b \in A$ if it exists, is well-defined upto a multiplication by a unit and is denoted by $\gcd(a,b)$ (resp. $\operatorname{lcm}(a,b)$).

From the characterisation of the divisibility 1.A. in factorial rings, we have:

1.A.17 Theorem Let A be a factorial ring and let $a, b \in A$. Then gcd (resp lcm) of a and b exists. Moreover, if P is a representative system for the classe of prime elements in A, then:

$$\gcd(a,b) = \prod_{p \in P} p^{\operatorname{Min}(v_p(a),\, v_p(b))}$$ and

$$\operatorname{lcm}(a,b) = \prod_{p \in P} p^{\operatorname{Max}(v_p(a),\, v_p(b))}$$

1.A.18 Rules for gcd Let A be an integral domain with gcd (i.e. gcd of any two elements in A exists). Then for $a, b, c \in A$, we have:

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

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

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

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

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

Proof An easy exercise.

The associativity property (3) of gcd allows us to define gcd of a finite subset of A:

Let $a_1, \cdots, a_n \in A$, $n \geq 0$ be elements in an integral domain. An element $d \in A$ is called a gcd of $a_1, \cdots, a_n$ and is denoted by $\gcd(a_1, \cdots, a_n)$ if

(1) $d|a_1, \cdots, d|a_n$ and (2) if $t \in A$ and $t|a_1, \cdots, t|a_n$, then $t|d$.

The element d (if it exists) is uniquely determined by $a_1, \cdots, a_n$, upto a multiplication by a unit in A.

Similarly, we can define lcm of $a_1, \cdots, a_n \in A$, $n \geq 0$, denoted by $\mathrm{lcm}(a_1, \cdots, a_n)$.

Convention $\gcd(\phi) = 0$ and $\mathrm{lcm}(\phi) = 1$.

1.A.19 Definition Let $a_1, \cdots, a_n \in A$, $n \geq 1$ be elements in an integral domain. We say that $a_1, \cdots, a_n$ are relatively prime if $\gcd(a_1, \cdots, a_n) = 1$. We say that $a_1, \cdots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ for every $1 \leq i, j \leq n$, $i \neq j$.

<u>Proof</u> (1) is immediate by definition. (2) is clear from $a \mid \gcd(a,b) \iff a \mid b$.

(3) Let $d = \gcd(a,b)$, $x = \gcd(d,c)$, $y = \gcd(b,c)$ and $z = \gcd(a,y)$. We need to show that $x \mid z$ and $z \mid x$. By definition

$$x \mid d \quad \text{and} \quad x \mid c$$

Then, since $d \mid a$ and $d \mid b$, we have
$x \mid a$, $x \mid b$ and $x \mid c$.

Therefore $x \mid a$ and $x \mid \gcd(b,c) = y$. Then $x \mid \gcd(a,y) = z$. Similarly $z \mid \gcd(d,c) = x$.

(4) Let $d = \gcd(a,b)$ and $e = \gcd(ca, cb)$. We need to show that $cd \mid e$ and $\underline{e \mid cd}$. Wma $c \neq 0$ (~~This is trivial~~ for $c = 0$, since $e = \gcd(0,0) = 0$)

$d \mid a$ and $d \mid b \Rightarrow cd \mid ca$ and $cd \mid cb \Rightarrow cd \mid \underbrace{\gcd(ca, cb)}_{=e}$,

i.e. $\underline{e = cdf}$ for some $f \in A$

$e \mid ca$ and $e \mid cb \Rightarrow ca = er$ and $cb = es$ for some $r, s \in A$

$\Rightarrow ca = er = cdf r$, $cb = es = cdfs$ $\Rightarrow$ $a = dfr$, since ($c \neq 0$) and $b = dfs$.
[illegible] in A

$\Rightarrow df \mid a$ & $df \mid b \Rightarrow df \mid \gcd(a,b) = d$

~~$df = da$~~ ~~$d = (df)g$~~
~~for some $g \in A$~~

$\Rightarrow \underbrace{cdf}_{e=} \mid cd$.

1A/16b

(5) $\cancel{\gcd(a,c)\cdot b = \gcd(ab, cb)}$.

~~Since~~ $\cancel{\gcd(cb, c) = c}$ ~~by (2), we have by (3)~~

$\gcd(\gcd(a,c)\cdot b, c) \overset{(4)}{=} \gcd(\gcd(ab, cb), c) \overset{(3)}{=}$

$\gcd(ab, \gcd(cb, c)) \overset{(2)}{=} \gcd(ab, c)$

1.A.20 Lemma Let A be an integral domain with gcd and let $a, b \in A$ be two relatively prime elements in A. Suppose that $a | bc$, $c \in A$. Then $a | c$.

Proof Since $a | bc$, we have $\gcd(a, bc) = a$ by (2) of 1.A. Now, using $\gcd(b, a) = 1$ and the product rule (s of 1.A. , we get $a = \gcd(bc, a) = \gcd(\gcd(b,a)c, a) = \gcd(c, a)$, in particular, $a | c$.

1.A.21 Remark. The above proof does not use the structure of ideals in A. It is not analogous to the usual proof in the case when $A = \mathbb{Z}$ or a PID, where ideal-theoretic argument with a representation $1 = ra + sb$ for some $r, s \in \mathbb{Z}$ is used.

1.A.22 Corollary Let A be an integral domain with gcd. Then every irreducible element in A is prime.

Proof It is enough to show that if $p \in A$ is irreducib and if $p | ab$, then either $p | a$ or $p | b$. Suppose that $p \nmid b$, i.e. $\gcd(p, b) \neq p$ by rule (2) of 1.A. and hence $\gcd(p, b) = 1$, since p is irreducible in A. Now, $p | a$ by 1.A.

Below we give ideal-theoretic description for gcd and lcm:

1.A.23 Lemma Let A be an integral domain and let $a_1, \cdots, a_n \in A$. Then:

(1) $\mathrm{lcm}(a_1, \cdots, a_n)$ exists if and only if the ideal $Aa_1 \cap \cdots \cap Aa_n$ is a principal ideal in A. Moreover, in this case every generator of this ideal is a lcm of $a_1, \cdots, a_n$.

(2) If $Aa_1 + \cdots + Aa_n$ is a principal ideal in A, then every generator of this ideal is a gcd of $a_1, \cdots, a_n$.

Proof (1) Let $\mathfrak{a} = Aa_1 \cap \cdots \cap Aa_n$. Then a generator of $\mathfrak{a}$ is an element which divisible by every element of $\mathfrak{a}$ and which is also minimum with respect to the divisibility. From this (1) is immediate.

(2) Suppose that $Aa_1 + \cdots + Aa_n = Ad$. Then $a_i \in Ad$ i.e. $d \mid a_i$ for every $i = 1, \cdots, n$. If $t \mid a_i$ for every $i = 1, \cdots, n$, then $a_i \in At$ for every $i = 1, \cdots, n$ and so $Ad = Aa_1 + \cdots + Aa_n \subseteq At$, i.e. $t \mid d$.

1.A.24 Example Let A be an integral domain. For the existence of gcd of $a_1, \cdots, a_n \in A$, it is not necessary that the ideal $Aa_1 + \cdots + Aa_n$ is principal in A. For example, the ring $\mathbb{Z}[X]$ is a factorial domain and hence $\gcd(2, X) = 1$ exists, but simple calculation on degrees, show that the ideal $2\mathbb{Z}[X] + X\mathbb{Z}[X]$ is not principal (see).
Therefore $\mathbb{Z}[X]$ is an example of a factorial domain, which is not a PID.