1. Basic notions:

We investigate number theory in *integral domains* (ID), i.e. in commutative rings R with identity and without zero-divisors.

Units are the divisors of all elements.

Two elements differing only in a unit factor are called *associates*, this means that they are mutual divisors of each other.

An element p is *irreducible* if p is not zero and not a unit, and $p = ab \Rightarrow a$ or b is a unit.

An element q is a *prime* if q is not zero and not a unit, and $q \mid cd \Rightarrow q \mid c$ or $q \mid d$.

A *greatest common divisor* $\gcd\{a, b\}$ of a and b is a common divisor which is a multiple of all common divisors of a and b. The definition implies that any two gcd-s are associates.

An ID is a *unique factorization domain* (UFD), if every non-zero and non-unit element has a factorization into the product of irreducible elements and this is unique apart from associates and the order of the factors.

2. Connection with ideals

Theorem 1

(i) $c \mid d \iff d \in (c) \iff (d) \subseteq (c)$;

(ii) c and d are associates iff $(c) = (d)$;

(iii) $(d) = (a, b) \Rightarrow d = \gcd\{a, b\}$;

(iv) $(d) = (a, b) \iff [d = \gcd\{a, b\}$ and $d = au + bv$ for some $u, v \in R]$.

Proof:

(i) is clear from the definitions and (ii) follows from (i).

Turning to (iii), $a \in (a, b) = (d) \Rightarrow d \mid a$, and similarly $d \mid b$, so d is a common divisor of a and b. If c is any common divisor, then $c \mid a \Rightarrow a \in (c)$, and similarly $b \in (c)$, thus $(d) = (a, b) \subseteq (c)$, since (a, b) is the smallest ideal containing a and b. Hence, $c \mid d$. — Note that the converse is false, e.g. 2 and x are coprime in $\mathbf{Z}[x]$, but $(1) \neq (2, x)$.

Finally, in (iv), $d \in (d) = (a, b)$ implies $d = au + bv$ and we saw in (iii) that $d = \gcd\{a, b\}$. Conversely, $d = au + bv \Rightarrow d \in (a, b)$, so $(d) \subseteq (a, b)$. On the other hand, $d \mid a \Rightarrow a \in (d)$, similarly $b \in (d)$, so $(a, b) \subseteq (d)$.

3. UFD

Theorem 2

An integral domain R is a UFD iff

(i) a strictly increasing sequence

$$(a_1) \subset (a_2) \subset \ldots \subset (a_j) \subset \ldots$$

of principal ideals cannot be infinite; and

(ii) every irreducible element is a prime.

Proof: We prove first the sufficiency of conditions (i) and (ii).

Uniqueness follows from (ii): Let (*) $a = p_1 \ldots p_k = q_1 \ldots q_t$ where p_i and q_j are irreducible elements. We have to show that $k = t$ and reordering suitably the factors, p_i and q_i are associates for every i. If the latter is true for some but not all i, then we can cancel with these pairs (and the remaining unit factor can be absorbed into one of the remaining irreducible factors). Hence, we may assume that no p_i and q_j are associates in (*). Now, $p_1 \mid q_1 \dots q_t$, so by (ii), $p_1 \mid q_j$ for some j. But q_j is irreducible, thus p_1 is a unit or an associate of q_j, and both are impossible.

We shall use (i) to establish decomposability. Let a be an arbitrary element in R different from 0 and units. As a first step, we show that a has an irreducible divisor.

If a is irreducible, we are done. Otherwise, $a = a_1 b_1$, where none of a_1 and b_1 is a unit. Then $(a) \subset (a_1)$ by Theorem 1 with a strict containment, as b_1 is not a unit.

If a_1 is irreducible, then it is an irreducible divisor of a. Otherwise, $a_1 = a_2 b_2$, where none of a_2 and b_2 is a unit. Then $(a_1) \subset (a_2)$ (with a strict containment).

We show that continuing the procedure similarly, some a_i is necessarily irreducible. Indeed, if this were not the case, then

$$(a) \subset (a_1) \subset \dots \subset (a_j) \subset \dots$$

would be an infinite strictly ascending chain of principal ideals, contradicting thus (i). Herewith we have proved that a has an irreducible divisor.

Now we show that a can be written as the product of irreducible elements. If a is irreducible, then we are done. Otherwise, $a = p_1 c_1$, where p_1 is irreducible and c_1 is not a unit. Since p_1 is not a unit either, so $(a) \subset (c_1)$ (with a strict containment).

If c_1 is irreducible, then both factors in $a = p_1 c_1$ are irreducible and we are done. Otherwise, $c_1 = p_2 c_2$, where p_2 is irreducible and c_2 is not a unit. Thus $(c_1) \subset (c_2)$ (with a strict containment).

Continuing the procedure similarly, some c_i is necessarily a unit, since otherwise the infinite strictly ascending chain

$$(a) \subset (c_1) \subset \dots \subset (c_j) \subset \dots$$

contradicts condition (i). This means that we arrived at a decomposition of a into the product of irreducible elements.

Turning to necessity, assume that R is a UFD. To prove (ii), let p be irreducible and $p \mid cd$ i.e. $ph = cd$. Factoring h, c, and d into irreducible factors, we have to arrive at essentially the same factorization on the two sides of $ph = cd$. As p occurs in the factorization of the LHS, so its associate must appear also among the irreducible factors on the RHS. But these factors come from c and d, so p must divide (at least) one of c and d.

Finally, to prove (i) by contradiction, assume the existence of an infinite strictly increasing chain

$$(a_1) \subset (a_2) \subset \dots \subset (a_j) \subset \dots$$

of principal ideals. Here $a_2 \neq 0$, and $a_3, a_4, \dots$ are infinitely many, pairwise non-associate divisors of a_2. But this is impossible, since if $a_2 = p_1 \dots p_k$, where every p_i is irreducible, then unique factorization implies that every divisor of a_2 is either a unit, or an associate of the product of some factors p_i (and if a_2 is a unit, then so are all its divisors, too).

4. Principal ideal domain (PID)

R is a *principal ideal domain* (PID) if every ideal in R is a principal ideal.

Theorem 3

A PID is a UFD.

Note that the converse is false, e.g. $\mathbf{Z}[x]$ is a UFD but not a PID.

Proof: We verify that a PID satisfies conditions (i) and (ii) of Theorem 2.

(i) To achieve a contradiction, assume the existence of an infinite strictly increasing chain

$$(a_1) \subset (a_2) \subset \ldots \subset (a_j) \subset \ldots$$

of principal ideals. A simple calculation shows that $A = \bigcup_{j=1}^{\infty}(a_j)$ is an ideal. As R is a principal ideal domain, therefore also A is a principal ideal, $A = (b)$. Then

$$b \in A = \bigcup_{j=1}^{\infty}(a_j),$$

so $b \in (a_k)$, i.e. $(b) \subseteq (a_k)$ for some k. Thus

$$A = (b) \subseteq (a_k) \subset (a_{k+1}) \subset \bigcup_{j=1}^{\infty}(a_j) = A,$$

a contradiction.

(ii) We verify first that any two elements a and b have a greatest common divisor. Since also (a,b) is a principal ideal (d), Theorem 1 implies $d = \gcd\{a,b\}$.

Let now p be irreducible and $p \mid ab$. Then $\gcd\{a,p\} = 1$ or p. In the latter case $p \mid a$. In the first case, $p \mid ab$ and $p \mid pb$ imply $p \mid \gcd\{ab, pb\} = b \cdot \gcd\{a,p\} = b$.

5. Euclidean domain (ED)

An integral domain R is a *Euclidean domain* (ED) if we can assign to every $c \in R \setminus \{0\}$ a non-negative integer $f(c)$ so that to every $a, b \in R$, $b \neq 0$ there exist $q, r \in R$ satisfying (**) $a = bq + r$ and $f(r) < f(b)$ or $r = 0$.

Examples: In $\mathbf{Z}$, we can choose $f(c) = |c|$; in $F[x]$ where F is a field, we can take $f(c) = \deg c$; in the ring of Gaussian integers $f(c) = N(c)$ works.

Theorem 4

A ED is a PID, hence also a UFD.

Proof: We have to verify that every ideal I of R is a principal ideal.

If the only element in I is 0, then $I = (0)$. Otherwise, consider the values $f(c)$ assigned to the non-zero elements of I. These are non-negative integers, thus there must be a smallest among them, let this be $f(b)$ (here b is not unique in general). We prove $I = (b)$.

As $b \in I$, thus $(b) \subseteq I$. Conversely, let a be an arbitrary element in I. We have to show $a \in (b)$, i.e. $b \mid a$.

We apply the division algorithm for a and b: there exist q, $r \in R$ satisfying (**). Since a, $b \in I$ and I is an ideal, so $r = a - bq \in I$. Further, $f(b)$ was minimal, so $f(r) < f(b)$ is impossible, hence $r = 0$, i.e. $b \mid a$, indeed.

freud@caesar.elte.hu