COURSE 8

Unique factorization domains

We remind a result concerning posets, result which will prove to be very useful for characterizing the class of integral domains we will introduce in this course.

Theorem 1. The following conditions are equivalent for a poset $(A, \leq)$:
1) **The minimal condition**: Any nonempty subset $B \subseteq A$ has a minimal element.
2) If $B \subseteq A$ fulfills the following conditions:
   α) B contains all the minimal elements of A;
   β) $a \in A$ and $\{x \in A \mid x < a\} \subseteq B \Rightarrow a \in B$,
then $B = A$.
3) **The descending chain condition** (abreviated **DCC**): any descending chain of elements of A,

$$a_1 > a_2 > \cdots > a_n > \dots\ ,$$

is finite. (Equivalently, this means that for any chain

$$a_1 \geq a_2 \geq \cdots \geq a_n \geq \dots$$

from A, there exists an index m such that $a_m = a_{m+1} = \dots$.)

The condition 2) of the previous theorem is a version of transfinite induction. The theorem determines the class of posets for which one can use this induction.

In the following part of the course, $(R, +, \cdot)$ will denote an integral domain.

Definition 2. Let $a \in R$, $x_i \in R$, $(i = 1, \dots, k)$, $y_j \in R$ $(j = 1, \dots, n)$ and

$$a = x_1 \cdots x_k = y_1 \cdots y_n$$

two factorizations of a. We say that these factorizations are **associated** if $k = n$ and, after a suitable change of the indexes of the second factorization, we have $x_i \sim y_i$ for all $i = 1, \dots, n$.

Example 3. If $1 = u_1 \dots u_k$ in R then the factorizations $a = x_1 \cdots x_k$ and $a = (u_1x_1) \cdots (u_kx_k)$ are associated.

Definition 4. An integral domain $(R, +, \cdot)$ is a **unique factorization domain** (abreviated **UFD**) or a **factorial domain** if any $a \in R^*$ which is not a unit can be written as a product of irreducible elements and any two factorizations of a as products of irreducible elements are associated.

Example 5. From the Fundamental Theorem of Arithmetic it follos that $(\mathbb{Z}, +, \cdot)$ is a UFD.

If one drops in the previous definition the request for any two factorizations of a non-zero non-unit element to be associated, one gets a class of integral domains which strictly includes the unique factorization domains.

Definition 6. An integral domain R is an **atomic domain** if any $a \in R^*$ which is not a unit can be written as a product of irreducible elements.

Remarks 7. ... and some examples ...
a) If for an integral domain R there exists a mapping $\varphi : R^* \to \mathbb{N}$ such that

$$a, b \in R^*,\ b \mid a,\ a \nmid b \Rightarrow \varphi(b) < \varphi(a), \tag{$*$}$$

then R is an atomic domain.
b) Using a), one can easily prove that $K[X]$ (with K field) and $\mathbb{Z}[\sqrt{d}]$ (with $d \in \mathbb{Z} \setminus \{1\}$ square-free integer) are atomic domains. For $K[X]$, φ can be considered to be the degree function (i.e. $f = \deg$) and for $\mathbb{Z}[\sqrt{d}]$, one can take φ to be the norm map δ.
c) The integral domain $\mathbb{Z}[X]$ is an atomic domain. Yet, for proving this, we cannot consider $\varphi = \deg : \mathbb{Z}[X] \setminus \{0\} \to \mathbb{N}$ since $(*)$ is not valid for this function. Indeed, in $\mathbb{Z}[X]$, $X \mid (2X)$, $(2X) \nmid X$, but $\deg X = 1 = \deg(2X)$.
d) Any UFD is an atomic domain, but there exist atomic domains which are not UFDs. From b) it follows that $\mathbb{Z}[i\sqrt{5}]$ is an atomic domain. But $\mathbb{Z}[i\sqrt{5}]$ is not a UFD ($6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ are non-associated factorizations of 6 in $\mathbb{Z}[i\sqrt{5}]$).

Theorem 8. If R is a UFD then:
1) The poset $(R^*/\sim, \leq)$ satisfies the minimality condition, i.e. any nonempty subset of $R^*/\sim$ has a minimal element.
2) Any two elements of R have a gcd.

Theorem 9. An integral domain R is a UFD if and only if the following conditions hold for R:
1) The poset $(R^*/\sim, \leq)$ satisfies the minimality condition.
2$'$) Any irreducible element of R is prime.

Folosind teorema 9 din cursul 7 se constată imediat că:

Corollary 10. An integral domain R is a UFD if and only if the following conditions hold for R:
1) The poset $(R^*/\sim, \leq)$ satisfies the minimality condition.
2) Any two elements of R have a gcd.

Remarks 11. a) For proving that $(\mathbb{Z}[i\sqrt{5}], +, \cdot)$ is not a UFD one can also use theorem 9 and the example 11 of Course 7.
b) The condition 1) from theorems 8 and 9 can be rewritten as follows: *for any sequence*

$$x_1, x_2, \dots, x_n, \dots$$

from R for which $x_{i+1} \mid x_i$ for any $i \in \mathbb{N}^*$, there exists $k \in \mathbb{N}^*$ such that $x_i \sim x_k$ for all $i \geq k$.

Theorem 12. Any PID is a UFD.

Remarks 13. a) In the next course we will deal with a subclass of the class of PIDs (which contains $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{R}[X]$ and $\mathbb{C}[X]$). This class will help us extend the list of examples of PIDs and UFDs.
b) There exist UFDs which are not PIDs. In one of the courses concerning the divisibility in rings of polynomials, we will prove that $\mathbb{Z}[X]$ is an example in this respect.