COURSE 9

Euclidean domains

Definition 1. An integral domain R is an **Euclidean domain** if there exists a map $\delta : R^* \to \mathbb{N}$ which satisfies the following condition: for any $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that

$$a = bq + r, \text{ where } r = 0 \text{ or } \delta(r) < \delta(b). \qquad (*)$$

Example 2. 1) From the integer division algorithm one deduces that $\mathbb{Z}$, with the absolute value mapping $\delta : \mathbb{Z} \to \mathbb{N}$, $\delta(n) = |n|$ is an Euclidean domain.
2) The Gauss integers domain $\mathbb{Z}[i]$, with the norm map $\delta : \mathbb{Z}[i] \to \mathbb{N}$, $\delta(z) = |z\overline{z}|$, is an Euclidian domain.

Remark 3. In the Euclidean domain definition, the existence of $q, r \in R$ which satify $(*)$ does not imply, in general, their uniqueness. For instance, for $\mathbb{Z}$ and the absolute value map, we have:

$$-4 = 3(-1) + (-1), \text{ with } 1 = |-1| < |3| = 3,$$
$$-4 = 3(-2) + 2, \text{ with } 2 = |2| < |3| = 3.$$

Obviously, only the second equality provides us with the quotient and the remainder of the division of -4 by 3 in $\mathbb{Z}$.

Theorem 4. If R is an Euclidean domain, then R is a PID.

Corollary 5. If R is an Euclidean domain, then R is a UFD.

Remark 6. As in the 4th course, one can show that the usual addition and multiplication provide $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] = \left\{a + b \cdot \frac{1+i\sqrt{19}}{2} \,\middle|\, a, b \in \mathbb{Z}\right\}$ with an integral domain structure. In the Appendix of the Romanian version you can find a quite elementary proof for the fact that $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ is a PID which is not an Euclidean domain.

From corollary 5 one deduces that if (R, δ) is an Euclidean domain then any $a, b \in R$ have a gcd. As for integers, we can use the **Euclid's algorithm** for finding a gcd of a and b in R. If one of the elements $a, b \in R$ is zero then the other element is a gcd. If $a \neq 0$ and $b \neq 0$, then there exist $q_1, r_1 \in R$ such that $a = bq_1 + r_1$, where $r_1 = 0$ or $\delta(r_1) < \delta(b)$. If $r_1 \neq 0$, then there exist $q_2, r_2 \in R$ such that $b = r_1q_2 + r_2$ where $r_2 = 0$ or $\delta(r_1) > \delta(r_2)$. If $r_2 \neq 0$, the algorithm continues and it provides us with a decreasing chain of natural numbers $\delta(r_1) > \delta(r_2) > \cdots$. Since such a chain has to be finite, in a certain number of steps, say $n + 1$, we get $r_{n+1} = 0$, so the algorithm gives us a finite sequence of equalities:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n-1} \end{aligned} \qquad (**)$$

where $r_i \neq 0$, $i = 1, \ldots, n$.

Theorem 7. If (R, δ) is an Euclidean domain and $a, b \in R^*$, then r_n from the equalities $(**)$ is the gcd of a and b.

Remark 8. If R is an Euclidean domain and d is a gcd for a and b, then there exist $u, v \in R$ such that $d = au + bv$, and we can use the Euclid's algorithm for finding u and v.

In the next course we will discuss some details concerning the arithmetic of polynomial rings. An important tool in this respect is **the division algorithm for polynomials** over fields:

Theorem 9. Let K be a field. For any $f, g \in K[X]$, $g \neq 0$ there exist $q, r \in K[X]$, uniquely determined, such that

$$f = gq + r \text{ and } \deg r < \deg g.$$

Corollary 10. Let K be a field and $c \in K$. The remainder of $f \in K[X]$ when divided by $X - c$ is $f(c)$.

Corollary 11. Let K be a field. An element $c \in K$ is a root of f if and only if $(X - c) \mid f$.

Corollary 12. If K is a field then any non-zero polynomial $f \in K[X]$ of degree k has at most k roots in K.

Corollary 13. Let K be a field. From theorem 9 it follows that the domain $K[X]$, with the degree function $\delta : K[X]^* \to \mathbb{N}$, $\delta(f) = \deg f$, is an Euclidean domain.

Example 14. We can use the Euclid's algorithm to show that in $\mathbb{Q}[X]$ the polynomials

$$f = X^3 - 6X^2 + 9X + 3 \text{ and } g = X^2 - 6X + 8$$

are coprime and also to show that for the polynomials $u = -\frac{1}{35}(X - 9)$ and $v = \frac{1}{35}(X^2 - 9X + 1)$, the equality $uf + vg = 1$ holds.