COURSE 10

Divisibility in polynomial rings

Some properties concerning the divisibility in polynomial rings were previously presented as examples or exercises. We assume them to be known when starting this section and we plan to present some details concerning this topic (e.g. the fact that $\mathbb{Z}[X]$ is a UFD which is not a PID).

Let R be an integral domain. We remind that $R[X]$ is also an integral domain and that the units of $R[X]$ are exactly the units of R. Consequently, the polynomials $f, g \in R[X]$ are associates if and only it there exists a unit $a \in R^*$ such that $f = ag$.

Remarks 1. a) From the distributivity of the multiplication with respect to the addition of $R[X]$ it follows that if $b \in R$ and $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ then

$$b \mid f \Leftrightarrow b \mid a_i,\ \forall i \in \{0, \ldots, n\}.$$

b) Since $U(R[X]) = U(R)$, one deduces easily that if $a \in R^*$ is an irredicible element of R then a is also irreducible in $R[X]$.
c) If $p \in R^*$ is a prime element in R then p is also prime in $R[X]$.

Definition 2. Let R be a UFD. The **content of a polynomial** is the gcd of its coefficients. A polynomial $\varphi \in R[X]$ is **primitive** if its content is 1.

Remarks 3. i) If $f \in R[X]^*$ and a is the content f then

$$f = a\varphi, \tag{1}$$

where φ is a primitive polynomial.
ii) Any associate of a primitive polinomial is also primitive.
iii) A zero degree polynomial is primitive if and only if it is a unit. Consequently, any nonzero polynomial over a field K is primitive.
iv) The representation (1) of f is unique up to a multiplication of its content by a unit of R.

Lemma 4. (**Gauss's Lemma**) If R is a UFD, the product of a two primitive polynomials from $R[X]$ is a primitive polynomial.

Corollary 5. a) If for $f \in R[X]$ we denote the content of f by $c(f)$, then

$$c(f_1f_2) = c(f_1)c(f_2),\ \forall f_1, f_2 \in R[X].$$

b) If $a_1, a_2 \in R^*$ and $\varphi_1, \varphi_2 \in R[X]$ are primitive polynomials, then

$$a_1\varphi_1 \mid a_2\varphi_2 \Leftrightarrow a_1 \mid a_2 \text{ and } \varphi_1 \mid \varphi_2.$$

At the end of the previous course we saw that for a field K, the polynomial ring $K[X]$, with the corresponding degree function, is an Euclidean domain (hence also a PID and a UFD) because of **the division algorithm for polynomials** over K: *for any polynomials $f, g \in K[X]$, $g \neq 0$, there exist the uniquely determined polynomials $q, r \in K[X]$ such that $f = gq + r$ and $\deg r < \deg g$.*

What if $R[X]$ is a polynomial ring over an integral domain R which is not a field? Definitely, $R[X]$ is no longer an Euglidean domain, since — as the next theorem shows — it is not a PID.

Theorem 6. If R is an integral domain which is not a field then $R[X]$ has non-principal ideals.

Corollary 7. The ring $\mathbb{Z}[X]$ of the polynomials with integer coefficients is not a PID.

But *if R is a UFD then $R[X]$ is also a UFD.* The proof of this statement is actually developed in the ring of polynomials over the fraction field of R. In the romanian (extended) version of the course we proved this statemen for $\mathbb{Z}[X]$ and the provided proof can easily be used for the general case (if one replaces $\mathbb{Q}$ — which is the fraction field of $\mathbb{Z}$ — by the fraction field of R). Actually, in the next part of the course we refer, mainly, to the ring $\mathbb{Z}[X]$.

Remarks 8. i) Let $f \in \mathbb{Z}[X]$ with $\deg f \geq 1$. Then f is irreductible in $\mathbb{Z}[X]$ if and only if f is irreducible in $\mathbb{Q}[X]$ and primitive in $\mathbb{Z}[X]$.
ii) The ring $\mathbb{Z}[X]$ is an example of UFD which is not a PID.

In $\mathbb{Z}[X]$ the prime elements and the irreducible elements coincide. A sufficient condition for an element of $\mathbb{Z}[X]$ to be irreducible(=prime) is given by the following statement.

Eisenstein's Criterion. Let $n \in \mathbb{N}^*$ and let

$$f = a_0 + \cdots + a_{n-1}X^{n-1} + a_nX^n \in \mathbb{Z}[X]$$

be a primitive polynomial. If there exists a prime number p such that

$$p \mid a_0, \ldots, p \mid a_{n-1} \text{ and } p^2 \nmid a_0$$

then the polynomial f is irreducible over $\mathbb{Z}$ (hence also over $\mathbb{Q}$).

Remarks 9. a) Using Eisenstein's Criterion, one can prove that for any $n \in \mathbb{N}^*$, the polynomial $f = X^n + 2$ is irreducible in $\mathbb{Z}[X]$, thus also in $\mathbb{Q}[X]$. If $p \in \mathbb{Z}$ is a prime then p is irreducible in $\mathbb{Z}[X]$, but not in $\mathbb{Q}[X]$.
b) Although the irreducible polynomials of $\mathbb{C}[X]$ are the degree 1 polynomials and in $\mathbb{R}[X]$ there is no irreducible polynomial with the degree greater than 2, the remark a) shows that in $\mathbb{Q}[X]$ one can find irreducible polynomials of any degree $n \in \mathbb{N}^*$, and in $\mathbb{Z}[X]$ one can find irreducible polynomials of any degree $n \in \mathbb{N}$.