LECTURE 11.

ALIREZA SALEHI GOLSEFIDY

1. Ring of polynomials.

For any ring R, we can consider the ring of polynomials $R[x]$ with coefficients in R. So by the definition

$$R[x] := \{a_0 + a_1x + a_2x^2 + \cdots + c_nx^n \; a_i \in R\},$$

and two polynomials $p(x) := \sum_i a_ix^i$ and $\sum_j b_jx^j$ are called to be equal if (and only if) for any i we have $a_i = b_i$.

Warning: Though for any $p(x) \in R[x]$ we can and will talk about the value of $p(a)$ for any $a \in R$, the ring of polynomials are not functions on R. The following example clarifies this point:

Example 1. *Let $p(x) = x^3 - x \in \mathbb{Z}/3\mathbb{Z}[x]$. Then for any $a \in \mathbb{Z}/3\mathbb{Z}$ we have that $p(a) = 0$. But $p \neq 0$ as a polynomial.*

Example 2. *Let $p(x) = x^3 - x, q(x) = x^3 - 3x^2 + x \in \mathbb{Z}/3\mathbb{Z}[x]$. Then $q(x) = p(x)$ as two polynomials.*

Example 3. *If R has characteristic p, where p is prime, then $(x + 1)^p = x^p + 1$.*

Definition 4. Let $p(x) = \sum_i a_ix^i$. Let n be the largest integer such that $a_n \neq 0$, then n is called the degree of p and is denoted by $\deg(p)$. a_n is called the leading coefficient. a_0 is called the constant term. If the leading coefficient is one, p is called a monic polynomial. The degree of the zero polynomial is defined to be $-\infty$.

Lemma 5. *Let R be an integral domain. Then $\deg(pq) = \deg(p) + \deg(q)$ and $R[x]$ is also an integral domain.*

Example 6. *Lemma 5 does not hold for an arbitrary ring. For instance let $p(x) = 2x + 1,\ q(x) = 2x^2 + 3 \in \mathbb{Z}/4\mathbb{Z}[x]$. Then $\deg(pq) = 2 \neq \deg(p) + \deg(q)$.*

Example 7. *If R is an integral domain and $\mathrm{char}(R) = p$ where p is prime, then $(x+1)^{p-1} = \sum_{i=0}^{p-1}(-1)^ix^i$. Hence for any prime p and $0 \leq i < p$, we have*

$$\binom{p-1}{i} \equiv (-1)^i \pmod{p}.$$

By Lemma 5 $R[x]$ is an integral domain. So it has cancellation property. On the other hand by Example 3 we have

$$(x + 1) \cdot (x + 1)^{p-1} = (x + 1)^p = x^p + 1 = (x + 1) \cdot (\sum_{i=0}^{p-1}(-1)^ix^i).$$

Theorem 8 (Division algorithm)**.** *Let F be field, $f(x), g(x) \in F[x]$. Assume that $g(x) \neq 0$. Then there are unique polynomials $q(x), r(x) \in F[x]$ such that*

(1) $f(x) = g(x)q(x) + r(x)$,
(2) $\deg(r) < \deg(g)$.

Date: 2/6/2012.

Mathematics Dept, University of California, San Diego, CA 92093-0112

E-mail address: golsefidy@ucsd.edu