Lecture notes Abstract Modern Algebra: Lecture 21

1 Rings of polynomials

In this section we shall assume that R is a commutative ring with identity. Any expression of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

where $a_i \in R$ and $a_n \neq 0$, is called a **polynomial** over R with indeterminate x. The elements $a_0, a_1, \ldots, a_n$ are called the coefficients of f. The coefficient a_n is called the **leading coefficient**. A polynomial is called monic if the leading coefficient is 1. If n is the largest nonnegative number for which $a_n \neq 0$, we say that **the degree of** f is n and write $\deg f(x) = n$. If no such n exist, the polynomial is called the zero polynomial and the degree is defined to be $-\infty$.
The ring of polynomials with coefficients in R is denoted by $R[x]$. For any polynomials $f(x), g(x)$, we have the following properties

1. For $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} a_i x^i$, the product $f(x)g(x)$ is defined by

$$f(x) \cdot g(x) = \sum_{i=0}^{n+m} c_i x^i,$$

   where $c_i = \sum_{j=0}^{i} a_j b_{i-j}$.

2. As a consequence of the previous property $\deg(f(x)g(x)) = \deg(f(x)) \cdot \deg(g(x))$, **as long as R is an integral domain**.

3. On the other hand, for the sum and the difference

$$\deg(f(x) \pm g(x)) \leq \max(\deg(f(x)) \deg(g(x))).$$

Remark 1. We can not expect $R[x]$ to be an integral domain if R is not an integral domain. The product of two non-zero polynomials can be the zero polynomial. Consider, for example, the polynomials

$$p(x) = 3 + 3x^3 \qquad \text{and} \qquad q(x) = 4 + 4x^2 + 4x^4.$$

We can check that $p(x)q(x) = 0$ in $\mathbb{Z}_{12}$. In particular, in this case, the degree $\deg p(x)q(x) \neq \deg p(x) + \deg q(x)$.

On the other hand, we expect some good properties:

Theorem 2. *Let R be a commutative ring with identity. Then $R[x]$ is a commutative ring with identity.*

Proof. Our first task is to show that $R[x]$ is an abelian group under polynomial addition. The zero polynomial, $f(x) = 0$, is the additive identity. Given a polynomial $p(x) = \sum_{i=0}^{n} a_i x^i$, the inverse of $p(x)$ is easily verified to be $-p(x)$. Commutativity and associativity follow immediately from the definition of polynomial addition and from the fact that addition in R is both commutative and associative. □

Theorem 3. *(**Evaluation homomorphism**) Let R be a commutative ring with identity and $\alpha \in R$. Then we have a ring homomorphism $\varphi_\alpha \colon R[x] \longrightarrow R$ defined by*

$$\varphi_\alpha(p(x)) = p(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0,$$

for $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

Proof. Let $p(x) = \sum_{i=1}^{n} a_i x^i$ and $q(x) = \sum_{j=1}^{m} b_j x^j$. It is easy to show that the evaluation on the sum $\varphi_\alpha(p(x)+q(x)) = \varphi_\alpha(p(x)) + \varphi_\alpha(q(x))$. To show that multiplication is preserved under the map φ_α, observe that

$$\varphi_\alpha(p(x)q(x)) = \sum_{i=1}^{n} a_i\alpha^i \cdot \sum_{j=1}^{m} b_j\alpha^j = \varphi_\alpha(p(x)) \cdot \varphi_\alpha(q(x))$$

The map $\varphi_\alpha \colon R[x] \longrightarrow R$ is called the evaluation homomorphism at α. □

Question 4. What is the kernel of the map φ_α?

To be answer that question we will work first over a field F. For polynomials with coefficients in a field, we can do a division algorithm similar to the one we do with integers.

Theorem 5. *(**Division Algorithm**) Let F be a field. Let $f(x)$ and $g(x)$ be polynomials in $F[x]$, where F is a field and $g(x)$ is a nonzero polynomial. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that*

$$f(x) = g(x)q(x) + r(x),$$

where either $\deg r(x) < \deg g(x)$ or $r(x)$ is the zero polynomial.

Proof. The proof is analogous to the proof on integers with the degree of the polynomial playing the role of the absolute value. We proceed using induction on the degree. Suppose that $f(x)$ is not the zero polynomial and that $\deg f(x) = n$ and $\deg g(x) = m$. If $m > n$, then we can let $q(x) = 0$ and $r(x) = f(x)$. Hence, we may assume that $m \leq n$ and proceed by induction on n. If $f(x) = \sum_{i=1}^{n} a_i x^i$ and $g(x) = \sum_{j=1}^{m} b_j x^j$, the polynomial

$$f'(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$

has degree less than n or is the zero polynomial. By induction, there exist polynomials $q'(x)$ and $r(x)$ such that

$$f'(x) = q'(x)g(x) + r(x),$$

where $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x)$. Now let

$$q(x) = q'(x) + \frac{a_n}{b_m}x^{n-m}$$

Then

$$f(x) = g(x)q(x) + r(x),$$

with $r(x)$ the zero polynomial or $\deg r(x) < \deg g(x)$. The uniqueness of the the polynomials $q(x), r(x)$ is proved by contradiction, since the existence of two different pairs q_1, r_1 and q_2, r_2, will give an equation of the sort

$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x),$$

where $r_1 - r_2$ is a polynomial of degree less than $\deg g(x)$. This forces $r_1(x) = r_2(x)$ and $q_1(x) = q_2(x)$. □

Now, we are in position of describing the kernel of the map $\varphi_\alpha \colon F[x] \to F$:

Corollary 6. *Let F be a field. An element $\alpha \in F$ is a zero of $p(x) \in F[x]$ if and only if $x - \alpha$ is a factor of $p(x)$ in $F[x]$. In other words, the kernel $\ker(\varphi_\alpha)$ of the map $\varphi_\alpha \colon F[x] \to F$ is the ideal $I_\alpha = \langle x - \alpha \rangle$.*

Proof. Suppose that $\alpha \in F$ and $p(\alpha) = 0$. By the division algorithm, there exist polynomials $q(x)$ and $r(x)$ such that

$$p(x) = (x - \alpha)q(x) + r(x)$$

and the degree of $r(x)$ must be less than the degree of $x - \alpha$. Since the degree of $r(x)$ is less than 1, the polynomial $r(x)$ must be a constant $r(x) = a$ for element $a \in F$; therefore,

$$p(x) = (x - \alpha)q(x) + a.$$

But $0 = p(\alpha) = 0 \cdot q(\alpha) + a = a$ and consequently, $p(x) = (x - \alpha)q(x)$, and $x - \alpha$ is a factor of $p(x)$. Conversely, suppose that $x - \alpha$ is a factor of $p(x)$; say $p(x) = (x - \alpha)q(x)$. Then $p(\alpha) = 0$. □

Remark 7. The division algorithm does not work when we are not over a field, for example, we cannot find $q(x)$ and $r(x)$ for $f(x) = x^2 - 5$ and $g(x) = 2x + 1$ in $\mathbb{Z}[x]$. The division algorithm by monic polynomials does work over all rings. So, if α is a root of a polynomial $p(x) \in R[x]$ then $p(x) = (x - \alpha)q(x)$ If the number $\beta \neq \alpha$ is another root of p, then $(\beta - \alpha)q(\beta) = 0$. Unfortunately, we cannot conclude that $q(\beta) = 0$, because $\beta - \alpha$ might be a zero divisor in R.

Corollary 8. *Let F be a field. A nonzero polynomial $p(x)$ of degree n in $F[x]$ can have at most n distinct zeros in F.*

Proof. We will use induction on the degree of $p(x)$. If $\deg p(x) = 0$, then $p(x)$ is a constant polynomial and has no zeros. Let $\deg p(x) = 1$. Then $p(x) = ax + b$ for some values of $a, b \in F$. If the α_1 and α_2 are both zeroes, we get $\alpha_1 = \alpha_2$.
Now assume that $\deg p(x) > 1$. If $p(x)$ does not have a zero in F, then we are done. On the other hand, if α is a zero of $p(x)$, then $p(x) = (x-\alpha)q(x)$ for some $q(x) \in F[x]$. The degree of of the polynomial $q(x)$ is $n-1$. Let β be some other zero of $p(x)$ that is distinct from α. Then $p(\beta) = (\beta - \alpha)q(\beta) = 0$. Since $\alpha \neq \beta$ and F is a field, we must have $q(\beta) = 0$. By our induction hypothesis, $q(x)$ can have at most $n-1$ zeros in F that are distinct from α. Therefore, $p(x)$ has at most n distinct zeros in F. □

Remark 9. The inequality in the previous corollary is necessary. The field of real numbers $F = \mathbb{R}$ has polynomials, like $p(x) = x^2 + 1$ **with no-real roots**.

Definition 10. A field F such **any polynomial of degree** n with coefficients in F has exactly n zeroes is called **an algebraically closed field**.

Example 11. The field of real numbers $\mathbb{R}$ **is not algebraically closed**. The field of complex numbers is algebraically closed, although we are not going to prove it here.