Elements of Algebraic Structures March 12 2024

Lecture 13: Ideals, Quotient rings

Lecture: Sujata Ghosh *Scribe: Sandeep Chatterjee*

1 Topics for this lecture

In this lecture, we shall talk about the following

1. Polynomial Rings
2. Monic Polynomials
3. The Fundamental Theorem of Algebra

2 Polynomial Rings

Let us first consider polynomial rings where the underlying ring is a field, F, say.
Consider $F[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in F \forall i, \text{ and } n \geq 0\}$.
We have: $(F[x], +, \cdot)$ forms a ring.

Properties of Polynomial Rings

Theorem 2.1 *Let $[R; +, \cdot]$ be a ring. Then:*

1. *$R[x]$ is a ring under the operations of polynomial addition and multiplication.*
2. *If R is a commutative ring, then $R[x]$ is a commutative ring.*
3. *If R is a ring with unity, 1, then $R[x]$ is a ring with unity (the unity in $R[x]$ is $1 + 0x + 0x^2 + \dots$).*
4. *If R is an integral domain, then $R[x]$ is an integral domain.*
5. *If F is a field, then $F[x]$ is not a field. However, $F[x]$ is an integral domain.*

Solved Exercise:
Let $f(x) = 1 + x$ and $g(x) = 1 + x + x^2$. Compute the following sums and products in the indicated rings:

1. $f(x) + g(x)$ and $f(x) \cdot g(x)$ in $\mathbb{Z}[x]$
2. $f(x) + g(x)$ and $f(x) \cdot g(x)$ in $\mathbb{Z}_2[x]$
3. $(f(x) \cdot g(x)) \cdot f(x)$ in $\mathbb{Q}[x]$
4. $(f(x) \cdot g(x)) \cdot f(x)$ in $\mathbb{Z}_2[x]$
5. $f(x) \cdot f(x) + f(x) \cdot g(x)$ in $\mathbb{Z}_2[x]$

Answers:

1. $f(x) + g(x) = 2 + 2x + x^2$, $f(x) \cdot g(x) = 1 + 2x + 2x^2 + x^3$
2. $f(x) + g(x) = x^2$, $f(x) \cdot g(x) = 1 + x^3$
3. $1 + 3x + 4x^2 + 3x^3 + x^4$
4. $1 + x + x^3 + x^4$
5. $x^2 + x^3$

The Factor Theorem

Theorem 2.2 *Let $[F; +, \cdot]$ be a field. An element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $x - a$ is a factor of $f(x)$ in $F[x]$.*

Proof:
($\Rightarrow$) Assume that $a \in F$ is a zero of $f(x) \in F[x]$. We wish to show that $x-a$ is a factor of $f(x)$. To do so, apply the division property to $f(x)$ and $g(x) = x-a$. Hence, there exist unique polynomials $q(x)$ and $r(x)$ from $F[x]$ such that $f(x) = (x-a)\cdot q(x)+r(x)$ and $\deg(r(x)) < \deg(x - a) = 1$, so $r(x) = c \in F$, that is, $r(x)$ is a constant. Also, the fact that a is a zero of $f(x)$ means that $f(a) = 0$. So $f(x) = (x - a) \cdot q(x) + c$ becomes $0 = f(a) = (a - a)q(a) + c$. Hence $c = 0$, so $f(x) = (x - a) \cdot q(x)$, and $x - a$ is a factor of $f(x)$. The reader should note that a critical point of the proof of this half of the theorem was the part of the division property that stated that $\deg(r(x)) < \deg(g(x))$.
($\Leftarrow$) It has been left to the reader as the next exercise.

Exercise : Prove the converse of The Factor Theorem - (Theorem 2.2) ($\Leftarrow$)

From The Factor Theorem, 2.2, we can get yet another insight into the problems associated with solving polynomial equations; that is, finding the zeros of a polynomial.

The initial important idea here is that the zero a is from the ground field F. Second, a is a zero only if $(x-a)$ is a factor of $f(x)$ in $F[x]$; that is, only when $f(x)$ can be factored (or reduced) to the product of $(x-a)$ times some other polynomial in $F[x]$.
What about the ideals in this ring?
Let us introduce the concept of monic polynomials.

Definition 2.3 *A **monic polynomial** is a polynomial where the coefficient of the highest power is* 1.

Of course, any polynomial over a field can be reduced to a monic polynomial.
To view the definitions alternatively,
Let $n \in \mathbb{Z}^+ \cup \{0\}$ be a non-negative integer, and let $a_0, a_1, \ldots, a_n \in \mathbb{C}$ be complex numbers. Then we call the expression

$$p(z) = a_n z^n + \ldots + a_1 z + a_0 \tag{2.2.1}$$

a polynomial in the variable z with coefficients $a_0, a_1, \ldots, a_n$. If $a_n \neq 0$, then we say that $p(z)$ has degree n (denoted $\deg(p(z)) = n$), and we call a_n the leading term of $p(z)$. Moreover, if $a_n = 1$, then we call $p(z)$ a monic polynomial. If, however, $n = a_0 = 0$, then we call $p(z) = 0$ the zero polynomial and set $\deg(0) = -\infty$.
Finally, by a root (a.k.a. zero) of a polynomial $p(z)$, we mean a complex number z_0 such that, upon setting $z = z_0$, we obtain the zero polynomial $p(z_0) = 0$. Note, in particular, that every complex number is a root of the zero polynomial.
Convention dictates that

- a degree zero polynomial be called a constant polynomial,
- a degree one polynomial be called a linear polynomial,
- a degree two polynomial be called a quadratic polynomial,
- a degree three polynomial be called a cubic polynomial,
- a degree four polynomial be called a quadric polynomial,
- a degree five polynomial be called a quintic polynomial, and so on.

Continuing with the notion of polynomials, let's see an example
Example:

$$f(x) = x^3 + 2x^2 + 3x + 7$$
$$g(x) = x^2 + x + 1$$

So, $\deg g < \deg f$. Then there exist polynomials $q(x)$ and $r(x)$, such that

$$f(x) = g(x) \cdot q(x) + r(x)$$

with $\deg r < \deg g$.
Question: If we take $q(x) = x$, would this result be satisfied? No.
Question: If we take $q(x) = x + 1$, would this result be satisfied? Yes.

Result: Given any two polynomials f and g over a field F with $\deg g \leq \deg f$, there exist polynomials $q(x)$ and $r(x)$, such that

$$f(x) = g(x) \cdot q(x) + r(x)$$

with $\deg r < \deg g$.

3 The Fundamental Theorem of Algebra

Theorem 3.1 *Every ideal $\mathcal{O} \neq I \subset F[x]$ is a principal ideal generated by a monic polynomial f in I of minimal degree.*

Proof. We have $\mathcal{O} \neq \{0\}$. Let $f(x) \in I$ be a monic polynomial of minimal degree. Now, consider any $h(x) \in I$. So, we have $h(x) = f(x) \cdot q(x) + r(x)$, with $\deg r < \deg f$.
Then, $r(x) = h(x) - f(x) \cdot q(x) \in I$. Thus, $r(x) \in I$ and $\deg r < \deg f$.
So, $r(x) = \{0\}$ (why?). Then, $h(x) = q(x) \cdot f(x)$.
So, I is generated by $f(x)$, i.e., $I = (f(x))$. This completes the proof. □

The Fundamental Theorem of Algebra

The statement of the Fundamental Theorem of Algebra found mostly on common textbooks, can also be read as follows: Any non-constant complex polynomial function defined on the complex plane $\mathbb{C}$ (when thought of as $\mathbb{R}^2$) has at least one root, i.e., vanishes in at least one place. This version is very much specialized and not as ours earlier stated version, which is without the loss of generality. But, it is in this form that can be easily proved using Differential Calculus, with the help of the Extreme Value Theorem.
Given how long the Fundamental Theorem of Algebra has been around, you should not be surprised that there are many proofs of it. There have even been entire books devoted solely to exploring the mathematics behind various distinct proofs. Different proofs arise from attempting to understand the statement of the theorem from the viewpoint of different branches of mathematics. This quickly leads to many non-trivial interactions with such fields of mathematics as Real and Complex Analysis, Topology, and (Modern) Abstract Algebra. The diversity of proof techniques available is yet another indication of how fundamental and deep the Fundamental Theorem of Algebra really is.
One such good general proof is being given in the next section.

4 Proof of the Fundamental Theorem of Algebra

Theorem 4.1 *Any polynomial of degree n has at most n roots.*

Proof. Let F be a field and $F[x]$ be the polynomial ring over F. Take any $\epsilon \in F$. We can define $h : F[x] \to F$ by $f(x) \mapsto f(\epsilon)$.
Question: Is h a homomorphism?

- $h(f_1(x) + f_2(x)) = f_1(\epsilon) + f_2(\epsilon) = h(f_1(x)) + h(f_2(x))$
- $h(f_1(x) \cdot f_2(x)) = f_1(\epsilon) \cdot f_2(\epsilon) = h(f_1(x)) \cdot h(f_2(x))$

Question: What is the kernel of h?

$$\text{Ker } h = \{f(x) \in F[x] : f(\epsilon) = 0\}$$

We have that Ker h forms an ideal of $F[x]$, and thus Ker h is a principal ideal generated by a monic polynomial of minimal degree.
Let us consider $x - \epsilon$, a monic polynomial. We have: $x - \epsilon \in$ Ker h. So, Ker $h = (x - \epsilon)$.
Take any $f(x) \in$ Ker h. So $f(\epsilon) = 0$.
Now, $f(x) = (x - \epsilon) \cdot g(x)$, where $g(x) \in F[x]$.
Now, suppose $f(x)$ is of degree n. Then, $g(x)$ is of degree $(n - 1)$.
So, by applying induction we can say that a polynomial of degree n has at most n roots.
This completes the proof. □