LECTURE 13 12.03.2024

Polynomial rings

Let us first consider polynomial rings where the underlying ring is a field, F, say.

Consider $F[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n :$
$a_i \in F$ for all i, $n \geq 0\}$

We have: $(F[x], +, \cdot)$ forms a ring.

What about the ideals in this ring?

Let us introduce the concept of monic polynomials.

- 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.

An 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 $r(x)$, s.t.

$$f(x) = g(x) \cdot q(x) + r(x), \text{ with } \deg r < \deg g.$$

Q: If we take $q(x) = x$, would this result be satisfied? NO (Check!)

Q: If we take $q(x) = x + 1$, would this result be satisfied? YES (Check!)

Result: Given any two polynomials f and g over a field $\mathbb{F}$ with $\deg g \leq \deg f$, there exist polynomials $q(x)$ and $r(x)$, s.t.

$$f(x) = g(x) \cdot q(x) + r(x) \text{ with } \deg r < \deg g.$$

Theorem. Every ideal $\{0\} \neq I \subseteq F[x]$ is a principal ideal generated by a monic polynomial f in I of minimal degree.

Proof. We have: $I \neq \{0\}$. Let $f(x) \in I$ be a monic polynomial of minimal degree.

Now, consider any $h(x) \in I$. So, we have

$$h(x) = f(x) \cdot q(x) + r(x), \text{ with}$$

$$\deg r < \deg f.$$

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 $f(x)$, that is, $I = (f(x))$. This completes the proof.

Let us now try to provide another proof of the Fundamental Theorem of Algebra.

Fundamental Theorem of Algebra:

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 $c \in F$. We can define

$$h : F[x] \to F$$
$$f(x) \mapsto f(c).$$

Q. Is h a homomorphism?

- $h(f_1(x) + f_2(x)) = f_1(c) + f_2(c)$
$= h(f_1(x)) + h(f_2(x))$

- $h(f_1(x) \cdot f_2(x)) = f_1(c) \cdot f_2(c)$
$= h(f_1(x)) \cdot h(f_2(x)).$

Q. What is the kernel of h?

$\operatorname{Ker} h = \{ f(x) \in F[x] : f(c) = 0 \}.$

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 $x-c$, a monic polynomial. We have: $x-c \in \ker h$ and so, $\ker h = (x-c)$. Take any $f(x) \in \ker h$. So, $f(c) = 0$. Now $f(x) = (x-c) \cdot g(x)$, 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.

Note: The 'field' assumption is necessary.

Consider the polynomial x^2-1 over $\mathbb{Z}/8\mathbb{Z}$. It is a polynomial of degree 2, however, the roots are $[1]$, $[3]$, $[5]$ and $[7]$, that is, it has 4 roots in $\mathbb{Z}/8\mathbb{Z}$.