Lecture 16: More thorough study of ring of polynomials

In the previous lecture we saw the importance of having certain methods of finding out if a given polynomial is irreducible or not. So we focus on ring of polynomials for now. Recall

\[ \deg (a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0) = n \quad \text{if} \quad a_n \neq 0 \quad \text{and} \]

\[ \deg (0) = -\infty. \]

Then we proved:

**Lemma.** Suppose \( D \) is an integral domain. Then

\[ \forall f, g \in D[x], \quad \deg (fg) = \deg f + \deg g. \]

We were proving the following:

**Proposition.** Suppose \( D \) is an integral domain. Then

1. \( D[x] \) is an integral domain.
2. \( \mathcal{U}(D[x]) = \mathcal{U}(D) \); in particular, if \( F \) is a field, then \( \mathcal{U}(F[x]) = \{ f(x) \in F[x] \mid \deg f = 0 \} = F \setminus \{0\} \).

**Proof.** (1) Suppose to the contrary \( f, g \in D[x] \setminus \{0\} \) and \( fg = 0 \).

Then \( \deg f, \deg g \in \mathbb{Z}^\geq \), and \( \deg (fg) = -\infty \), which contradicts
the previous lemma.

2. Suppose \( f(x) \in U(D[x]) \). So \( \exists g(x) \in D[x] \) s.t.

\[ f(x) \cdot g(x) = 1. \]

Hence \( \deg f \cdot g = \deg 1 = 0 \), which implies

\[ a = \deg f + \deg g; \quad \text{and so} \quad \deg f = \deg g = 0. \]

Hence \( f(x) = a_0 \in D \) and \( g(x) = b_0 \in D \) and \( a_0 \cdot b_0 = 1 \).

Therefore \( a_0 \in U(D) \); this implies \( U(D[x]) \subseteq U(D) \). (I)

Since \( D \) is a subring of \( D[x] \), \( U(D) \subseteq U(D[x]) \). (II)

(I) and (II) imply \( U(D) = U(D[x]) \).

**Example.** \( U(Z[1x]) = U(Z) = \mathbb{Q} \pm i3 \)

\( U(\mathbb{Q}[1x]) = U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\} \)

**Example.** In \( Z_{16}[x] \), there are some non-constant units:

\( 1-2x \in U(Z_{16}[x]) \).

**Solution.** \( 1 = 1 - (2x)^4 = (1 - 2x)(1 + (2x) + (2x)^2 + (2x)^3) \).

The following is a good exercise:
Lecture 16: Factor theorem

\[a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{U}(\mathbb{R}[x]) \iff \exists a_0 \in \mathbb{U}(\mathbb{R}) \text{ and } a_1, \ldots, a_n \text{ are nilpotent} \]

that means \( a_i^m = 0 \).

(\iff) You can prove. (\iff) more tools are needed.

**Theorem.** Suppose \( F \) is a field, \( c \in F \), \( f(x) \in F[x] \). Then

\[ \exists q(x) \in F[x] \text{ st. } f(x) = (x - c) q(x) + f(c). \]

In particular, \( c \) is a zero of \( f \) if and only if \( \exists q(x) \in F[x] \)

\[ \text{st. } f(c) = q(x)(x-c). \]

**Pf.** By the long division, \( \exists q(x), r(x) \in F[x] \) st.

\[ f(x) = q(x)(x-c) + r(x) \text{ and } \deg r < \deg x-c = 1. \]

And so \( r(x) \)

is a constant polynomial. Evaluating at \( c \) we get

\[ f(c) = q(c)(c-c) + r(c) \implies r(c) = f(c). \]

Since \( r(x) \) is constant, \( r(x) = f(c) \). And so

\[ f(x) = q(x)(x-c) + f(c) \quad (I) \]

If \( c \) is a zero of \( f \), then \( f(c) = 0 \). Therefore by \( (I) \) \( f(x) = q(x)(x-c). \)

If \( f(x) = q(x)(x-c) \), then \( f(c) = q(c)(c-c) = 0 \).
Lecture 16: Number of zeros of a polynomial

Wednesday, May 9, 2018 5:03 PM

Proposition. Suppose \( F \) is a field, \( f(x) \in F[x] \) is a polynomial of degree \( n > 0 \).

(a) If \( c_1, \ldots, c_m \in F \) are distinct zeros of \( f \), then \( \exists g(x) \in F[x] \) s.t. \( f(x) = (x - c_1) \cdots (x - c_m) \ g(x) \).

(b) \( f(x) \) has at most \( n \) distinct zeros in \( F \).

\[ \begin{aligned}
\textbf{Proof.} \ (a) \text{ We proceed by induction on } m. \\
\underline{Base of induction.} \ m = 1. \text{ By the factor theorem, } \exists g(x) \in F[x], \ f(x) = (x - c_1) \ g(x). \\
\underline{Induction step.} \text{ Suppose } c_1, \ldots, c_{m+1} \text{ are distinct zeros in } F \text{ of } f(x). \text{ Then by the induction hypothesis, } \exists g(x) \in F[x] \text{ s.t.} \\
\begin{array}{c}
\text{(i) } f(x) = (x - c_1) \cdots (x - c_m) \ g(x) \ . \text{ And so} \\
\end{array}
\end{aligned} \]

\[ f(c_{m+1}) = ((c_{m+1} - c_1) \cdots (c_{m+1} - c_m) \ g(c_{m+1})) \]

Since \( F \) has no zero-divisors, \( g(c_{m+1}) \neq 0 \). Hence by the factor theorem \( \exists q(x) \in F[x], \ g(x) = (x - c_{m+1}) \ q(x) \). And so by (i)

\[ f(x) = (x - c_1) \cdots (x - c_m) (x - c_{m+1}) \ q(x). \]
(b) Suppose to the contrary that $\exists c_1, \ldots, c_{n+1}$ zeros of $f$.

Then by part (a), $f(x) = (x-c_1)(x-c_2)\ldots(x-c_{n+1})g(x)$ for some $g(x) \in \mathbb{F}[x]$.

And so $n = \deg f = \deg (x-c_1) + \ldots + \deg (x-c_{n+1}) + \deg g$

$= n + 1 + \deg g$.

Therefore $\deg g = -1$ which is a contradiction. \hfill \Box

Recall. Suppose $\text{Char}(\mathbb{R}) = p > 0$ is prime. Then $f: \mathbb{R} \to \mathbb{R}$, $f(r) = r^p$ is a ring hom. This is called the Frobenius map. Consider the Frobb. map $f: \mathbb{Z}_p \to \mathbb{Z}_p$, $f(r) = r^p$. Then for any $a \in \mathbb{Z}_p$,

$f(a) = f(\underbrace{1+\ldots+1}_a \text{ times}) = \underbrace{f(1)+\ldots+f(1)}_{a \text{ times}} = 1+\ldots+1 = a$ \($a$ times $a$ times $a$ times

$\Rightarrow a^p = a$.

Fermat’s little theorem. $\forall a \in \mathbb{Z}_p$, $a^p = a$.

Before this you have been working with polynomials in your calc. courses. But you mainly viewed them as functions. In this course
there is a subtle difference between a polynomial $f(x) \in \mathbb{F}_p$ and its underlying function. For instance $x$ and $x^p \in \mathbb{Z}_p[x]$ are two different polynomials one of them has degree 1 and the other one has degree $p$, but as functions from $\mathbb{Z}_p$ to $\mathbb{Z}_p$, they are equal as Fermat’s little theorem implies.