MA542 Lecture

Timothy Kohl

Boston University

February 5, 2025

Although we shall consider $R[x]$ for $R = \mathbb{Z}$ and other domains later, for now we want to examine $F[x]$ for F a field.

Also we shall introduce the following important concept which we shall elaborate on more later on in later sections.

Definition

Let $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ be rings, a function $\phi : R \to S$ is a ring homomorphism if
(i) $\phi(a +_R b) = \phi(a) +_S \phi(b)$
(ii) $\phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$
for all $a, b \in R$.

Here is a basic yet important example.

Define $\rho : \mathbb{Z} \to \mathbb{Z}_n$ be given by $\rho(a) = a \ mod \ n$ (i.e. remainder mod n), namely that if $a = qn + r$ then $\rho(a) = r$.

Verifying that ρ is a ring homomorphism is not extremely difficult, but a bit nit-picky.

We note

$$\rho((q_1 n + r_1) + (q_2 n + r_2)) = \rho(r_1 + r_2)$$

$$\rho((q_1 n + r_1)(q_2 n + r_2)) = \rho((q_1 q_2 n + q_1 r_2 + q_2 r_1)n + r_1 r_2) = \rho(r_1 r_2)$$

and so, one checks, for $r_1, r_2 \in \{0, \dots, n-1\}$ that $\rho(r_1 + r_2) = \rho(r_1) + \rho(r_2)$ and $\rho(r_1 r_2) = \rho(r_1)\rho(r_2)$.

Definition

If $\phi : R \to S$ is a ring homomorphism that is one-to-one and onto then we call it an isomorphism, and we write $R \cong S$, and say R is isomorphic to S.

We mention this definition to circle back briefly to the construction of $Frac(D)$ from a domain D.

Recall that $Frac(D) = \{\frac{a}{b} \mid a, b \in D, b \neq 0\}$ and we can define $\bar{D} = \{\frac{a}{1} \mid a \in D\} \subseteq Frac(D)$ then $\bar{D}$ is a subring of $Frac(D)$ as we saw earlier.

If we define $\phi : D \to \bar{D}$ by $\phi(a) = \frac{a}{1}$ then one can check that ϕ is a ring homomorphism, and that it is one-to-one and onto.

As such $D \cong \bar{D}$.

Now, let's get back to polynomials.

Theorem

If E is a field with a subfield $F \subseteq E$ and $\alpha \in E$ then the evaluation function

$$\phi_\alpha : F[x] \rightarrow E$$

given by $\phi_\alpha(f(x)) = f(\alpha)$ is a homomorphism.

Before we consider the proof, let's point out why we *don't* define $\phi_\alpha : F[x] \rightarrow F$.
The reason for this is that we want to consider polynomials with coefficients in a field F which may have roots which lie in some *larger* field E.
A basic example to consider is this $\phi_i : \mathbb{R}[x] \rightarrow \mathbb{C}$ where now $\phi_i(x^2+1) = i^2 + 1 = 0$.

Indeed this is one of the things we wish to understand, namely quantifying when a given polynomial with coefficients in F has roots in a larger field E.

Proof.

Let $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$ be polynomials in $F[x]$.

Then $\phi_\alpha(f(x)) = a_n\alpha^n + \cdots + a_0$ and since $\alpha \in E$ then $\alpha^i \in E$ and since $a_i \in F$ then $a_i \in E$ and so $a_i\alpha^i \in E$, so $f(\alpha) \in E$.

And so $\phi_\alpha(f(x) + g(x)) = (a_n\alpha^n + \cdots + a_0) + (b_m\alpha^m + \cdots + b_0)$ which we can easily see is equal to $\phi_\alpha(f(x)) + \phi_\alpha(g(x))$.

And similarly it's not hard to show $\phi_\alpha(f(x)g(x)) = \phi_\alpha(f(x))\phi_\alpha(g(x))$. $\square$

By looking at $\phi_\alpha : F[x] \to E$ for $F \subseteq E$ and $\alpha \in E$ we are looking towards questions about the solvability of equations.

In particular if $f(x) \in F[x]$, then $\alpha \in E$ is a <u>zero</u> or <u>root</u> of $f(x)$ if $\phi_\alpha(f(x)) = 0$, i.e. $f(\alpha) = 0$.

Example: Consider $\phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{R}$ and observe that for $f(x) = x^2 - 2$ we have $\phi_{\sqrt{2}}(f(x)) = 0$.

Moreover, and this is important, for **no** $\alpha \in \mathbb{Q}$ do we have that $\phi_\alpha(f(x)) = 0$.

i.e. $f(x) \in \mathbb{Q}[x]$ but $f(x) = 0$ has no solutions in $\mathbb{Q}$ but rather in a **larger** field containing $\mathbb{Q}$.

Moreover, if for $f(x) \in F[x]$ one has $f(x) = g(x)h(x)$ for polynomials $g(x), h(x) \in F[x]$ (i.e. $f(x)$ is factorable) then since ϕ_α is a homomorphism then we have

$$\phi_\alpha(g(x)h(x)) = \phi_\alpha(g(x))\phi_\alpha(h(x)) = g(\alpha)h(\alpha)$$

so that $\phi_\alpha(f(x)) = 0$ implies that $g(\alpha)h(\alpha) = 0$ which, since E is a field (and therefore a domain) means either $g(\alpha) = 0$ and/or $h(\alpha) = 0$.

Moreover, if $\alpha \in F$ then $\phi_\alpha(f(x)) = 0$ means α is a root of one of the factors of $f(x)$ in $F[x]$.

The following is fundamental to discussing the roots of a polynomial, and to understanding the structure of $F[x]$ as a ring.

Theorem (Division Algorithm)

Let F be a field, and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$, then there exists unique polynomials $q(x)$,$r(x)$ in $F[x]$ such that

$$f(x) = q(x)g(x) + r(x) \text{ think 'q' for quotient and 'r' for remainder}$$

where $deg(r(x)) < deg(g(x))$.

Note, it's possible (and indeed important to consider) the case where $r(x) = 0$.

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

PROOF: The proof is based on induction on $n = deg(f(x))$.

If $f(x) = 0$ or $deg(g(x)) > deg(f(x))$ then $q(x) = 0$ and $r(x) = f(x)$.

So if $deg(f(x)) = n$ and $deg(g(x)) = m$ where $n \geq m$ where say

$$f(x) = a_n x^n + \cdots + a_0$$
$$g(x) = b_m x^m + \cdots + b_0$$

then $a_n \neq 0$ and $b_m \neq 0$, and in particular $b_m^{-1} \in F$.

So let $t = n - m$ and define $q_1(x) = c_t x^t$ where $c_t = \frac{a_n}{b_m}$.

PROOF (continued) Then

$$\begin{aligned} q_1(x)g(x) &= (b_m \frac{a_n}{b_m})x^n + \dots \\ &= a_n x^n + \dots \end{aligned}$$

which means $deg(f(x) - q_1(x)g(x)) < n$ so by induction we may assume the theorem holds for $f(x) - q_1(x)g(x)$.

So there exists polynomials $q_2(x)$ and $r(x)$ such that $f(x) - q_1(x)g(x) = q_2(x)g(x) + r(x)$ which means

$$f(x) = (q_2(x) + q_1(x))g(x) + r(x) = q(x)g(x) + r(x)$$

i.e. $q(x) = q_1(x) + q_2(x)$ so that indeed, we have a quotient '$q(x)$' and a remainder '$r(x)$' so that $f(x) = q(x)g(x) + r(x)$.

PROOF (continued)

The last part to check is that if $f(x) = q(x)g(x) + r(x)$ and $f(x) = \tilde{q}(x)g(x) + \tilde{r}(x)$ that $\tilde{q}(x) = q(x)$ and $\tilde{r}(x) = r\,(x)$.

But this implies that

$$\begin{aligned} f(x) - f(x) &= (q(x)g(x) + r(x)) - (\tilde{q}(x)g(x) + \tilde{r}(x)) \\ &= (q(x) - \tilde{q}(x))g(x) + (r(x) - \tilde{r}(x)) \end{aligned}$$

but $f(x) - f(x) = 0$ so, by degree considerations $q(x) - \tilde{q}(x) = 0$ and $r(x) - \tilde{r}(x) = 0$ so $q(x) = \tilde{q}(x)$ and $r(x) = \tilde{r}(x)$. $\square$

What we've just done is basically 'polynomial long division'.
For example:

$$\begin{array}{r}
\frac{7}{2}x^2 \quad - x - \frac{9}{4} \\
2x^2+2x+1 \overline{\smash{\big)}\; 7x^4 + 5x^3 \quad - 3x^2 - 2x - 1} \\
\underline{-7x^4 - 7x^3 \quad - \frac{7}{2}x^2 \qquad\qquad} \\
-2x^3 - \frac{13}{2}x^2 - 2x \quad \\
\underline{2x^3 \quad + 2x^2 \quad + x \quad} \\
-\frac{9}{2}x^2 \quad - x - 1 \\
\underline{\frac{9}{2}x^2 + \frac{9}{2}x + \frac{9}{4}} \\
\frac{7}{2}x + \frac{5}{4}
\end{array}$$

Note, in the above example we have to be able to divide '2' into '7' to get the leading term $\frac{7}{2}x^2$ in the quotient, which explains why we insist on the polynomials being in $F[x]$ for F a field.

i.e. If we tried to do this in $\mathbb{Z}[x]$ say rather than $\mathbb{Q}[x]$ then it would fail since $q(x) = \frac{7}{2}x^2 - x - \frac{9}{4} \notin \mathbb{Z}[x]$.

Consequences of the Division Algorithm for $F[x]$

For $f(x), g(x) \in F[x]$ (where $g(x) \neq 0$) there exists a quotient $q(x)$ and remainder $r(x)$ where $f(x) = q(x)g(x) + r(x)$ where either $r(x) = 0$ or $deg(r(x)) < deg(g(x))$.

This mirrors the Division Algorithm in $\mathbb{Z}$ which says that for $a, m \in \mathbb{Z}$, if $m \neq 0$ then $a = qm + r$ for $0 \leq r \leq m - 1$.

There are a number of consequences of the division algorithm, some of which are familiar facts from high-school algebra.

Corollary

Let F be a field and $a \in F$ and if $f(x) \in F[x]$ then $f(a)$ is the remainder term in the division of $f(x)$ by $x - a$.

Proof.

Why? Well since $deg(x - a) = 1$ then when one divides $f(x)$ by $x - a$ the remainder must either be 0 or degree 0, i.e. a constant 'number' r.
So $f(x) = q(x)(x - a) + r$ and thus $f(a) = q(a)(a - a) + r$ i.e.
$f(a) = r$. □

From this we get other important facts.

Corollary

Let $f(x) \in F[x]$ then $a \in F$ is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

Proof.

Again if we divide $f(x)$ by $x - a$ then $f(x) = q(x)(x - 1) + r$ for a constant r (which could be zero).

So $f(a) = q(a)(a - a) + r = r$ so if $f(a) = 0$ then $r = 0$ and $f(x) = q(x)(x - a)$ (i.e. a multiple of $x - a$) and if $r \neq 0$ then $(x - a)$ does *not* evenly divide $f(x)$! $\square$