The evaluation homomorphisms

In the previous lecture we defined the evaluation at \( a \):

\[
\phi_a(f(x)) = f(a).
\]

Since both \( R[x] \) and \( R \) have distribution law, when \( R \) is a commutative ring, it is easy to see that

\[
\phi_a(f+g) = \phi_a(f) + \phi_a(g)
\]

and

\[
\phi_a(fg) = \phi_a(f) \phi_a(g);
\]

which means:

**Proposition.** Let \( R_1 \subseteq R_2 \) be commutative rings. Then for any \( a \in R_2 \), \( \phi_a : R_1[x] \to R_2, \phi_a(f) = f(a) \) is a ring homomorphism.

(Its proof is straightforward; justify this for yourself.)

**Ex.** The evaluation \( \phi_a \) at \( a \) maps \( a_0 + a_1x + \ldots + a_nx^n \) to the constant term. And so

\[
\ker \phi_a = \text{the set of multiples of } x.
\]

\[
= \{ a_0x + a_1x^2 + \ldots + a_nx^n \mid a_i \in R_2 \}.
\]
Ex. Give one non-zero element of $\ker(\phi_i)$ where

\[ \phi_i : \mathbb{Q}[x] \to \mathbb{C} \text{ is the evaluation at } i; \]

\[ \phi_i(f(x)) = f(i) \text{ where } i^2 = -1. \]

Solution. $f \in \ker(\phi_i) \iff f(i) = 0$.

So we need to find $f(x) \in \mathbb{Q}[x]$ s.t. $i$ is a zero of $f$. By the definition of $i$ we know that it is a zero of $x^2 + 1$. So $x^2 + 1 \in \ker \phi_i$. □

Ex. Find all $a \in \mathbb{C}$ s.t. $x^2 - x - 12 \in \ker \phi_a$ where

\[ \phi_a : \mathbb{Q}[x] \to \mathbb{C} \text{ is the evaluation at } a. \]

Solution. $x^2 - x - 12 \in \ker \phi_a \iff \phi_a(x^2 - x - 12) = 0$

\[ \iff a^2 - a - 12 = 0 \]

\[ \iff (a - 4)(a + 3) = 0 \text{ in } \mathbb{C} \text{ (and } \mathbb{C} \text{ is a field.)} \]

\[ \iff a = 4 \text{ or } a = -3. \] □

Ex. Find a non-zero element of $\ker(\phi_{\sqrt{2}})$ where

\[ \phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{C} \text{ is the evaluation at } \sqrt{2}. \]

Solution. $f \in \ker \phi_{\sqrt{2}} \iff f(\sqrt{2}) = 0$. 
The evaluation homomorphisms

Friday, August 18, 2017 12:54 AM

so we need to find a polynomial which has a zero at \( \sqrt{2} \).

By the definition of \( \sqrt{2} \), we have that it is a zero of \( x^2 - 2 \). So \( x^2 - 2 \in \ker \phi_{\sqrt{2}} \).

**Ex.** Is there a non-zero element in \( \ker \phi_{\pi} \) where \( \phi_{\pi} : \mathbb{Q}[X] \to \mathbb{C} \) is the evaluation at the \( \pi \)?

**Solution.** No, it is a not-so-easy theorem in number theory that \( \pi \) is NOT a zero of a polynomial with rational coefficients. Such a number is called a transcendental number.

**Def.** \( a \in \mathbb{C} \) is called **algebraic** if \( \ker \phi_a \not= \{0\} \)

where \( \phi_a : \mathbb{Q}[X] \to \mathbb{C} \) is the evaluation at \( a \).

- \( a \in \mathbb{C} \), which is not algebraic, is called a **transcendental number**.

**Ex.** Find \( \phi_2(x^{12} - x) \) where \( \phi_2 : \mathbb{Z}_{11}[X] \to \mathbb{Z}_{11} \)

is the evaluation at 2.

**Solution.** Since 11 is prime, \( \forall a \in \mathbb{Z}_{11}, \ a^{11} = a \).

So \( 2^{12} = 2^{11} \times 2 = 2 \times 2 \), which implies \( \phi_2(x^{12} - x) = 4 - 2 = 2 \).
The division algorithm

An extremely important property of ring of polynomials is the fact that we have a division algorithm:

\textbf{Theorem}. Suppose \( R \) is a unital commutative ring and \( 0 \neq 1 \). Let \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \) and \( g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0 \). Suppose \( b_m \in U(R) \).

Then \( \exists q(x) \in R[x] \) (called the quotient) and \( r(x) \in R[x] \) (called the remainder) s.t.

\begin{enumerate}
  \item \( f(x) = q(x) g(x) + r(x) \)
  \item \( \deg r < \deg g \).
\end{enumerate}

Moreover such pair \((q,r)\) is unique.

In class we proved the existence first and then showed the uniqueness when \( R \) is an integral domain.

\textit{Proof of existence}. We proceed by the strong induction on \( \deg(f) \). To do so first we have to address the case of \( f = 0 \).
Case of \( f=0 \). Set \( q=r=0 \). Then

1. \( \deg r=-\infty < m = \deg g \).
2. \( f=0 = 0 \times g + 0 \).

Base of induction. \( \deg f = 0 \). Then \( f(x)=a_0 \) and \( a_0 \neq 0 \).

Case 1. \( \deg g = m > 0 \).

Set \( q=0 \) and \( r(x)=a_0 \). Then

1. \( \deg r=0 < m = \deg g \).
2. \( f = a_0 = 0 \times g(x) + r \).

Case 2. \( \deg g = m = 0 \).

Then \( g(x) = b_0 \) and \( b_0 \in \text{V}(\mathbb{R}) \).

Set \( q(x)=a_0 b_0^{-1} \) and \( r(x)=0 \). Then

1. \( \deg r=-\infty < 0 = \deg g \).
2. \( f(x)=a_0 = (a_0 b_0^{-1}) b_0 + 0 \).

Strong induction step. Suppose for any polynomial of \( \deg < k \) we can find a quotient and a remainder, and we want to get the same result for \( f(x) \) with degree \( k \).

Case 1. \( \deg f=k < \deg g = m \).

Set \( q=0 \) and \( r(x)=f(x) \); check 1 and 2.
The division algorithm (existence)

Friday, August 18, 2017  12:53 PM

Case 2. \( \deg f = k \geq \deg g = m \).

So \( f(x) = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_0 \) and \( a_k \neq 0 \).

We look for a monomial, i.e. \( \Box x^\Box \), s.t. the leading term of \( \Box x^\Box \) \( g(x) \) is the same as the leading term \( a_k x^k \) of \( f(x) \).

That means we'd like to have \( (\Box x^\Box)(b_m x^m) = a_k x^k \).

So the monomial is \( a_{k-b_m-k-m} x^{k-m} \) (notice that \( k-m \geq 0 \), and so \( a_{k-b_m-k-m} x^{k-m} \) is a monomial). Hence

\[
\deg (f(x) - a_{k-b_m} x^{k-m} g(x)) < k.
\]

So by the strong induction hypothesis there are \( q_1(x), r_1(x) \in \mathbb{R}[x] \) s.t.

1. \( \deg r_1 < \deg g \),
2. \( f(x) - a_{k-b_m} x^{k-m} g(x) = q_1(x) g(x) + r_1(x) \).

2 implies that \( f(x) = (a_{k-b_m} x^{k-m} + q_1(x)) g(x) + r_1(x) \).

Let \( r(x) = r_1(x) \) and \( q(x) = a_{k-b_m} x^{k-m} + q_1(x) \).

Then 1 implies \( \deg r < \deg g \) and 2 gives us

\[
f(x) = q(x) g(x) + r(x).
\]
The division algorithm (uniqueness)

Proof of uniqueness. Suppose

1. \( \deg r_1, \deg r_2 < \deg g \)

2. \( f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x) \).

We have to show \( q_1 = q_2 \) and \( r_1 = r_2 \).

2. implies \( (q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x). \)

\[ \deg (r_2 - r_1) \leq \max(\deg r_1, \deg r_2) < \deg g. \]

Since the leading coefficient of \( g \) is a unit, we get

\[ \deg((q_1 - q_2)g) = \deg(q_1 - q_2) + \deg g \quad \text{(why?)} \]

(In class we proved this in integral domains.)

Hence \( \deg(q_1 - q_2) + \deg g = \deg(r_2 - r_1) < \deg g. \)

And so \( \deg(q_1 - q_2) < 0 \), which implies \( \deg(q_1 - q_2) = -\infty \)

and \( q_1 - q_2 = 0 \). Using \( \circ \) we get that \( r_2 - r_1 = 0. \)

So \( q_1 = q_2 \) and \( r_1 = r_2. \)

Next we use the division algorithm to study zeros of a polynomial.
The factor theorem

Theorem. Let $R$ be a unital commutative non-zero ring, and \( f(x) \in R[x] \). Then \( a \in R \) is a zero of \( f \) if and only if \( f(x) = (x-a)q(x) \) for some \( q(x) \in R[x] \).

Pf. ($\Rightarrow$) Since the leading coeff. of \( x-a \) is 1 and 1 \( \in \) \( U(R) \), by the division algorithm \( \exists \), \( q(x) \in R[x] \) s.t.

1. \( \deg r < \deg (x-a) = 1 \). \( \Rightarrow \) \( r \) is constant.

2. \( f(x) = (x-a)q(x) + r(x) \)

Since \( a \) is a zero of \( f \), \( \circ \) implies

\[ 0 = f(a) = (a-a)q(a) + r(a) \] ; and so \( r(a) = 0 \).

Since \( r \) is constant, we get that \( r(x) = r(a) = 0 \).

So \( f(x) = (x-a)q(x) \).

\( \Leftarrow \) \( f(x) = (x-a)q(x) \) implies \( f(a) = (a-a)q(a) = 0 \).

And so \( a \) is a zero of \( f \).

In the previous lectures we have seen that some degree 2 polynomials have more than 2 zeros. But this is not the
Zeros of a polynomial over an integral domain

Theorem. Let \( D \) be an integral domain, and \( f(x) \in D[x] \). Suppose \( a_1, \ldots, a_k \) are distinct zeros of \( f(x) \). Then

\[ \exists q(x) \in D[x] \text{ s.t. } f(x) = (x-a_1) \ldots (x-a_k) q(x). \]

In particular, a polynomial \( f \) has at most \( \deg(f) \) zeros.

**Proof.** We proceed by induction on \( k \).

**Base of induction.** \( k=1 \).

\( a_1 \) is a zero of \( f \). So by the factor theorem,

\[ f(x) = (x-a_1) q(x) \text{ for some } q(x) \in D[x]; \text{ this proves the base of induction.} \]

**Induction step.** Suppose \( a_1, \ldots, a_{k+1} \) are distinct zeros of \( f(x) \).

Since \( a_{k+1} \) is a zero of \( f \), by the factor theorem

\[ \exists h(x) \in D[x] \text{ s.t. } f(x) = (x-a_{k+1}) h(x). \text{ So, for any } 1 \leq i \leq k, \quad 0 = f(a_i) = (a_i-a_{k+1}) h(a_i). \text{ Since} \]

Zeros of a polynomial over an integral domain

\[ o = (a_i - a_{k+1}) \ h(a_i) \implies h(a_1) = h(a_2) = \ldots = h(a_k) = 0. \]

\[ a_i \neq a_{k+1} \text{ for } 1 \leq i \leq k \]

\[ D \text{ has no zero-divisor} \]

So \( a_1, \ldots, a_k \) are distinct zeros of \( h \). Hence by the induction hypothesis we have that

\[ h(x) = (x-a_1)(x-a_2) \ldots (x-a_k) q(x) \]

for some \( q(x) \in D[x] \). Therefore

\[ f(x) = (x-a_{k+1}) h(x) = (x-a_1)(x-a_2)(x-a_k) q(x). \]

This gives us the first part of the theorem.

To get the second part of the theorem, we have

\[ \deg f = \deg ((x-a_1)(x-a_2) q(x)) = k + \deg q, \]

which implies \( \deg f \geq k \). So \( f \) has at most \( \deg f \) zeros. \( \blacksquare \)