In the previous lecture we defined the ring of polynomials with coefficients in a ring $\mathbb{R}$ with an indeterminate $x$.

For $f(x) = \sum_{i=0}^{\infty} a_i \cdot x^i \in \mathbb{R}[x]$, we say

$$\deg f = \max \{ \xi \in \mathbb{Z}^+ \cup \{ -\infty \} \mid a_\xi \neq 0 \}.$$

So, the degree of the zero polynomial is defined to be $-\infty$; and

$$\deg (a_0 + a_1 x + \ldots + a_n x^n) = n \text{ if } a_n \neq 0.$$

**Ex.** $\deg (1) = 0$ in any (non-zero) unital ring.

**Ex.** Find $\deg ((2x^2 - 1)(2x + 1))$ in $\mathbb{Z}_4 [x]$.

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

$$= 2x^2 - 2x - 1.$$  

So $\deg ((2x^2 - 1)(2x + 1)) = 2$.

Notice that in the above example

$$\deg (2x^2 - 1) = 2, \quad \deg (2x + 1) = 1,$$ and

$$\deg ((2x^2 - 1)(2x + 1)) = 2 \neq 2 + 1 = \deg (2x^2 - 1) + \deg (2x + 1).$$

So, for a general ring $\mathbb{R}$, in $\mathbb{R}[x]$ we do not have

$$\deg (f \cdot g) = \deg f + \deg g.$$
A closer look at the previous example shows us why this equality fails; it fails because of the zero divisors. 

**Lemma.** Suppose \( R \) is a ring with no zero divisors. Then for any \( f, g \in R[X] \), we have 
\[
\deg fg = \deg f + \deg g.
\]

**Proof.** If either \( f \) or \( g \) is zero, then \( fg = 0 \). So the LHS = \(-\infty\) and the RHS = \(-\infty + \cdots = -\infty\) (as a convention: \(-\infty + n = -\infty\) and \((-\infty) + (-\infty) = -\infty\).)

Suppose \( f \) and \( g \) are not zero; and 
\[
f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \quad a_n \neq 0,
\]
\[
g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0, \quad b_m \neq 0.
\]

Then \( f(x) g(x) = a_n b_m x^{n+m} + \) (terms of degree < \( n+m \)).

Since \( a_n, b_m \neq 0 \) and \( R \) has no zero divisor, \( a_n b_m \neq 0 \). Hence 
\[
\deg fg = n+m = \deg f + \deg g.
\]

**Corollary.** If \( R \) has no zero divisors, then \( R[X] \) does not
Units of a ring of polynomials

Thursday, August 17, 2017 11:38 PM

has no zero divisors. If \( D \) is an integral domain, then \( D[x] \) is an integral domain.

**Proof.** If \( fg = 0 \), then \( \deg fg = -\infty \). Since \( R \) has no zero divisors, by Lemma, \( \deg fg = \deg f + \deg g \). Since two integers cannot add up to \(-\infty\), either \( \deg f = -\infty \) or \( \deg g = -\infty \); which implies either \( f = 0 \) or \( g = 0 \). Hence \( R[x] \) does not have a zero divisor.

If \( D \) is an integral domain, then

1. \( D \) is a non-zero unital ring \( \implies \ D[x] \) is a non-zero unital ring.
2. \( D \) is commutative \( \implies \ D[x] \) is commutative
3. \( D \) does not have a zero divisor \( \implies \ D[x] \) does not have a zero divisor.

Justify 1 and 2; 3 has been proved in the first part of this argument.

**Lemma** Suppose \( D \) is an integral domain. Then \( U(D[x]) = UD \).

**Proof.** Suppose \( f \in U(D[x]) \). Then \( \exists g \in D[x] \) s.t. \( fg = 1 \).
Since $D$ has no zero-divisors, we have

$$o = \deg fg = \deg f + \deg g.$$  

Notice that, since $fg \neq o$, $f$ and $g$ are NOT zero. So $\deg f, \deg g \geq 0$.

\[ \begin{align*}
\deg f + \deg g = 0 & \implies \deg f = \deg g = 0; \text{ so} \\
\deg f, \deg g & \geq 0 \\
\exists a_0, b_0 \in D \setminus \{0\} \text{ s.t. } f(x) = a_0 \text{ and } g(x) = b_0.
\end{align*} \]

Hence $a_0 b_0 = 1$, which implies $a_0 \in U(D)$. Therefore $f \in U(D)$; which implies $U(D[x]) \subseteq U(D)$.

Since $D$ and $D[x]$ have the same (multiplicative) identity, it is clear that $U(D) \subseteq U(D[x])$. Therefore by $\text{(i)}, \text{(ii)}$ one gets the claim.

**Ex.** $U(Z[x]) = \mathbb{Z}_4$; $U(Q[x]) = Q \setminus \{0\}$.

**Ex.** For a general ring $R$, $U(R[x])$ might be much larger than $U(R)$: show that $1 + 2x \in U(Z_4[x])$.

**Solution.** $(1 + 2x)(1 - 2x) = 1 - 2^2x^2 = 1 = (1 - 2x)(1 + 2x)$. ■
A closer look at the previous example shows that the key property is the fact that $2^2 = 0$ in $\mathbb{Z}_4$; we say 2 is a nilpotent element. In a ring $R$, an element $a \in R$ is called nilpotent if $\exists m \in \mathbb{Z}^+$ s.t. $a^m = 0$.

It is a good exercise to show that in a unital commutative ring $R$, we have

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

Prior to this course, you have viewed a polynomial $f \in R[x]$ as a function from $R$ to $R$. But there is a subtle difference between them. For instance there are only 4 functions from $\mathbb{Z}_2$ to $\mathbb{Z}_2$, but there are infinitely many polynomials in $\mathbb{Z}_2[x]$: $\deg(x^n) = n$ and so $x, x^2, x^3, \ldots$ are distinct polynomials ($\sum a_i x^i = \sum b_i x^i \iff \forall i, a_i = b_i$). They are however, equal as functions: $x \overset{\text{?}}{\longmapsto} x^n$.
Fermat's theorem

In fact we have:

**Theorem.** For any prime $p$ and $a \in \mathbb{Z}_p$, we have

$$a^p = a.$$

**Pf.** If $a = 0$, then $a^p = 0$; and there is nothing to prove.

If $a \neq 0$, then $a \in \mathbb{Z}_p^\times$, since $p$ is prime, $\gcd(a, p) = 1$. Hence $a \in \mathbb{U}(\mathbb{Z}_p)$. Therefore

$$\ell_a : \mathbb{Z}_p \to \mathbb{Z}_p, \quad \ell_a(b) = ab$$

is a bijection.

Hence $\{1, 2, \ldots, p-1\} = \{\ell_a(1), \ell_a(2), \ldots, \ell_a(p-1)\}$

$$\Rightarrow (p-1)! = \ell_a(1) \cdot \ell_a(2) \cdots \ell_a(p-1) \in \mathbb{Z}_p.$$

Since $1, 2, \ldots, p-1 \in \mathbb{U}(\mathbb{Z}_p)$, $(p-1)! \in \mathbb{U}(\mathbb{Z}_p)$. So we can cancel it out; and get $1 = a^{p-1} \in \mathbb{Z}_p$. Hence $a^p = a$.

So as two functions on $\mathbb{Z}_p$ we have $x^p = x$ but as two polynomials we have $x^p \neq x$.

Being aware of this issue, we still want to view a polyn.

as a function and **evaluate** it at a given point $a \in \mathbb{R}$. 
For $a \in \mathbb{R}$, let $\phi_a : \mathbb{R}[x] \to \mathbb{R}$ be

$$\phi_a(f(x)) = f(a).$$

It is called the evaluation at $a$; and we will study it in the next lecture.