Lecture 24 Unique factorization of polynomials over a field.

Let K be a field, $K[x]$ ring of polynomials

$f \in K[x]$ can be written $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ $(a_n \neq 0)$

we write $\deg f = n$. Then $\deg(fg) = \deg(f) + \deg(g)$

<u>Corollary</u>: $(K[x])^\times = K^\times = K \setminus \{0\}$. That is, the only polynomials that are invertible in $K[x]$ are the non-zero constant polynomials.

Proof Let $f, g \in K[x]$ be such that $fg = 1$ (so $f = g^{-1}, g = f^{-1}$)

Then $0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g)$

But $\deg(f)$ and $\deg(g)$ are both nonnegative.

$\therefore$ The only way for their sum to be zero is if both are zero.

So $f = a_0 \in K$ and $g = b_0 \in K$ and

$a_0 b_0 = 1$. So $a_0 \in K^\times$ and $b_0 \in K^\times$. ☒

<u>Def</u> A polynomial $f \in K[x]$ is <u>irreducible</u> if, whenever there is a factorization $f = gh$ for $g, h \in K[x]$, either $g \in K^\times$ or $h \in K^\times$ (either g or h is a constant). In otherwords, f cannot be factored into two polynomials of strictly smaller degree.

Examples $f = x^2+1$ is irreducible in $\mathbb{R}[x]$

But $x^2+1 = (x-i)(x+i)$ in $\mathbb{C}[x]$,

so it is not irreducible in $\mathbb{C}[x]$.

Moral: The choice of coefficient field matters!

Example $g = x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$ is reducible in $\mathbb{R}[x]$.

But it is irreducible in $\mathbb{Q}[x]$:

If $x^2-2 = (x-a)(x-b)$ with $a, b \in \mathbb{Q}$, then

substituting a for x gives $a^2-2=0$, which is impossible!

Example in $\mathbb{Z}_5[x]$, $h = x^2+[3]$ is irreducible

if $x^2+[3] = (x-[a])(x-[b])$

then $[a]^2+[3]=[0]$

so $[a]^2=[2]$

but $[0]^2=[0]$, $[1]^2=[1]$, $[2]^2=[4]$, $[3]^2=[9]=[4]$,

$[4]^2=[16]=[1]$, so $[a]^2=[2]$ is impossible!

<u>Theorem</u> (1.8.8, 1.8.21) Let $f \in K[x]$, $\deg(f) > 0$.
Then f can be factored into a product of irreducible polynomials
$$f = p_1 p_2 \cdots p_k \qquad p_i \in K[x] \text{ irreducible.}$$

The factorization is unique, up to reordering of the factors and multiplication by units: this means that if
$$f = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell \quad \text{are two factorizations}$$

with p_i and q_j irreducible, then $k = \ell$ and after reordering the factors we have $p_i = a_i q_i$ for $a_i \in K^\times$.

[Eg: $f = x^2 - 4 = (x-2)(x+2) = (2x+4)(\frac{1}{2}x - 1)$, $\quad (K = \mathbb{Q})$
but $2x+4 = 2(x+2)$ $\quad \frac{1}{2}x - 1 = \frac{1}{2}(x-2)$]

Remark: the proof is very similar to the factorization of integers $\mathbb{Z}$ but we use $\deg(f)$ instead of $|n|$.

<u>Proof of Existence</u>: Induction on $\deg(f)$.
Base case $\deg(f) = 1$. Then f is irreducible, for if $f = gh$, $1 = \deg(f) = \deg(g) + \deg(h)$
so either $\deg(g) = 0$ and $g \in K^\times$ or
$\deg(h) = 0$ and $h \in K^\times$.

Induction step: Assume existence of a factorization for all polynomials of degree $\leq n-1$. Let f have degree n. If f is irreducible, done. Otherwise, we can write
$$f = gh \quad \text{where } \deg(g) > 0 \text{ and } \deg(h) > 0.$$
Since $\deg(f) = \deg(g) + \deg(h)$, we must have

$$\deg(g) < \deg(f) = n \text{ and } \deg(h) < \deg(f) = n.$$

So by induction hypotheses, g and h are products of irreducibles, $g = p_1 p_2 \cdots p_r$ $\quad h = p_{r+1} p_{r+2} \cdots p_k$ (p_i irreducible)

and $f = gh = p_1 p_2 \cdots p_r p_{r+1} \cdots p_k$ is a product of irreducibles. $\boxtimes$

Uniqueness proof: deferred.

<u>Definition</u> Let $f, g \in K[x]$. We say f <u>divides</u> g, $f \mid g$, if there is $h \in K[x]$ such that $g = hf$.

<u>Proposition</u> (1.8.13) Let $f, d \in K[x]$. Then $\exists\, q, r \in K[x]$ such that
$$f = qd + r \text{ and } \deg(r) < \deg(d)$$

"Proof": long division of polynomials.

<u>Example</u>: In $\mathbb{Z}_3[x]$, $f = [2]x^5 + [1]x^2 + [2]x + [2]$
$\quad d = [2]x^2 + [1]$

Let's drop "$[\cdot]$".

$$\begin{array}{r l}
 & 1x^3 + 0x^2 + 1x + 2 \\
2x^2 + 0x + 1 & \overline{\big)\, 2x^5 + 0x^4 + 0x^3 + 1x^2 + 2x + 2} \\
 & -\underline{(2x^5 + 0x^4 + 1x^3)} \\
 & \qquad 2x^3 + 1x^2 + 2x + 2 \\
 & \qquad -\underline{(2x^3 + 0x^2 + 1x)} \\
 & \qquad\qquad 1x^2 + 1x + 2 \\
 & \qquad\qquad -\underline{(1x^2 + 0x + 2)} \\
 & \qquad\qquad\qquad 1x
\end{array}$$

so $q = [1]x^3 + [1]x + [2]$
$\quad r = [1]x$

Definition: A <u>gcd</u> of $f, g \in K[x]$ is an $h \in K[x]$ such that $h | f$ and $h | g$, and if $k \in K[x]$ is such that $k | f$ and $k | g$, then $k | h$ as well.
The gcd is not unique, but any two gcd's differ by multiplication by a unit $a \in K^\times$.
There is a unique gcd that is also <u>monic</u> (having leading coefficient 1). We denote it $\gcd(f, g)$

<u>Theorem</u> (1.8.16) For any $f, g \in K[x] \setminus \{0\}$, $\gcd(f, g)$ exists and $\exists s, t \in K[x]$ such that

$$\gcd(f, g) = sf + tg.$$

"<u>Proof</u>:" Iterated long division as in $\mathbb{Z}$.

Definition two polynomials f, g are <u>relatively prime</u> if $\gcd(f,g) = 1$

<u>Proposition</u>: If $p \in K[x]$ is irreducible, and $f | p$, then either $f \in K^\times$ or $f = ap$, where $a \in K^\times$.

<u>Proof</u> $f | p \Rightarrow p = fg$ since p irreducible, either $f \in K^\times$ or $g \in K^\times$ in latter case $f = g^{-1} p$, with $g^{-1} \in K^\times$.

<u>Proposition</u>: let $p \in K[x]$ be irreducible an let $f \in K[x]$. then either $p | f$ or $\gcd(p, f) = 1$.

<u>Proof</u>: If $\gcd(p, f) \neq 1$, there is $g \in K[x]$ with $\deg(g) > 0$ such that $g | p$ and $g | f$. thus by above $g = ap$ for some $a \in K^\times$. Also $f = gh = aph$ so $p | f$.

Proposition Let $p \in K[x]$ be irreducible and let $f, g \in K[x]$.
If $p | fg$, then either $p | f$ or $p | g$.

Proof: If $p | f$, we are done. If $p \nmid f$, $\gcd(p, f) = 1$, and we may write $1 = sp + tf$

then $g = spg + tfg$ since $p | spg$ and $p | tfg$ we find $p | g$ ∎.

Proof of essential uniqueness of factorization into irreducibles:
Suppose $f = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$

Since $p_1 | q_1 q_2 \cdots q_\ell$, $p_1 | q_j$ for some j. Then $p_1 = a_i q_j$ for $a_i \in K^\times$
Factor out p_1 and $a_i q_j$.

Then $p_2 p_3 \cdots p_k = a_i^{-1} q_1 q_2 \cdots \underset{\substack{\uparrow \\ q_j \text{ omitted}}}{\hat{q}_j} \cdots q_\ell = \frac{f}{p_1}$

a pair of factorizations of a lower degree polynomial.
proceed by induction.