9/19/2018
We
10.1

Last time: • Defined the ring of polynomials $K[x]$ with coefficients in $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

• defined degree of a polynomial.

Proved $\deg(f \cdot g) = \deg f + \deg g$ $(\deg 0 = -\infty)$

$\deg(f+g) \leq \max(\deg f, \deg g)$

Proved $\forall\ p, d \in K[x]$, $d \neq 0$ $\exists\ q, r \in K[x]$ so that

$$p(x) = q(x)\, d(x) + r(x) \quad \text{and} \quad \deg r < \deg d.$$

Ex

$$p(x) = 3x^3 + 3x^2 - x + 1 \qquad d(x) = x - 1 \qquad q(x)?\ \ r(x)?$$

Solution

$$\begin{array}{r|l} & 3x^2 + 6x + 5 \\ \hline x-1 & 3x^3 + 3x^2 - x + 1 \\ & 3x^3 - 3x^2 \\ \hline & \quad 6x^2 - x \\ & \quad 6x^2 - 6x \\ \hline & \qquad 5x + 1 \\ & \qquad 5x - 5 \\ \hline & \qquad\quad 6 \end{array}$$

$\Rightarrow$ $q(x) = 3x^2 + 6x + 5$

$r(x) = 6$.

Uniqueness Suppose $p(x) = q_1(x)\, d(x) + r_1(x) = q_2(x)\, d(x) + r_2(x)$

and $\deg r_1, \deg r_2 < \deg d$.

Then $(q_1(x) - q_2(x))\, d(x) = r_2(x) - r_1(x)$

$\Rightarrow$ $\deg(q_1 - q_2) + \deg d = \deg(r_2 - r_1) \leq \max(\deg r_2, \deg(-r_1))$

$< \deg d$.

$\Rightarrow$ $\deg(q_1 - q_2) < 0$

$\Rightarrow$ $\deg(q_1 - q_2) = -\infty$, i.e. $q_1 - q_2 = 0$

$\Rightarrow$ $r_2 - r_1 = (q_1 - q_2) \cdot d = 0 \cdot d = 0$.

---

Definition A polynomial $f(x) \in K[x]$ divides $g(x) \in K[x]$ iff there is $q(x) \in K[x]$ so that

$$g(x) = q(x) \cdot f(x).$$

We write $f \mid g$ if $f$ divides $g$ ( $g = qf$ for some $q$).

<u>Definition 1.8.23</u> $\alpha \in K[x]$ is a <u>root</u> of $f(x) \in K[x]$ if $f(\alpha) = 0$
(That is, if $f(x) = a_0 + a_1 x + \dots + a_n x^n$, we require that
$$a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n = 0$$
)

<u>Lemma 10.1</u> (compare with 1.8.22) $\alpha \in K$ is a root of $f(x) \in K[x]$
$\Leftrightarrow$ $x - \alpha \mid f(x)$.

<u>Proof</u> ($\Leftarrow$) if $x - \alpha \mid f(x)$, then $f(x) = (x-\alpha)\, q(x)$ for some $q(x) \in K[x]$. $\Rightarrow$ $f(\alpha) = (\alpha - \alpha) q(\alpha) = 0$ $\Rightarrow \alpha$ is a root of $f$.

($\Rightarrow$) By the devision algorithm
$$f(x) = (x-\alpha)\, q(x) + r(x) \quad \text{and } \deg r < \deg(x - \alpha) = 1$$
$\Rightarrow \deg r \leq 0$. $\Rightarrow$ $r(x) = r_0$ for some $r_0 \in K$.

Since $\alpha$ is a root of $f(x)$, $0 = f(\alpha)$.
$$\Rightarrow \quad 0 = f(\alpha) = (\alpha - \alpha)\, q(\alpha) + r_0 = 0 \cdot q(\alpha) + r_0 = r_0.$$
$$\Rightarrow \quad r_0 = 0. \quad \Rightarrow \quad (x - \alpha) \mid f(x) \qquad \square$$

---

The analogue of prime numbers in $K[x]$ are <u>irreducible polynomials</u>.

<u>Definition 1.8.7</u> A polynomial $f \in K[x]$ is <u>irreducible</u> if $\deg f > 0$ and $f$ cannot be written as a product of two polynomials of lower degree.

<u>Ex</u> In $K[x]$ any polynomial of degree 1 is irreducible.

$x^2 - 2 \in \mathbb{R}[x]$ is <u>not</u> irreducible $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

$x^2 - 2 \in \mathbb{Q}[x]$ <u>is</u> irreducible:

<u>If</u> $x^2 - 2 = f(x)\, g(x)$

then $f(x) = ax + b$ $g(x) = cx + d$ for some $a, b, c, d \in \mathbb{Q}$, with roots $-b/a$, $-d/c$

But $x^2 - 2$ has <u>no</u> roots in $\mathbb{Q}$: $\nexists\, e \in \mathbb{Q}$ s.t. $e^2 = 2$.

Fact (a theorem, which we won't prove ~~today~~)
Any polynomial $f(x) \in K[x]$ can be written as a product of irreducible polynomials, uniquely up to order of the factors.

Note if $p(x) \in K[x]$ is irreducible and $\deg p > 1$ then $p(x)$ has no roots in $K$.
Reason: If $p(x)$ has a root $\alpha \in K$ then $x - \alpha \mid p(x)$
$\Rightarrow$ $p(x) = (x-\alpha) q(x)$ for some $q(x) \in K[x]$
and $\deg q + 1 = \deg p$.
Impossible since $p$ is irreducible. $\Rightarrow$ $p$ has no roots.

Cor 1.8.24 Any polynomial $p(x) \in K[x]$ of degree $n \geq 1$ has at most $n$ roots (counted with multiplicities)

Proof Write $p(x)$ as a product of irreducibles:
$$p(x) = (x-\alpha_1)^{m_1} \cdots (x-\alpha_k)^{m_k} q_1(x) \cdots q_s(x)$$
where $q_1, \ldots, q_s$ are irreducible of degree $> 1$.
Note $q_j$'s have no roots in $K$ (see Note above)
If $\alpha$ is a root of $p(x)$ then
$$0 = p(\alpha) = (\alpha - \alpha_1)^{m_1} \cdots (\alpha-\alpha_k)^{m_k} q_1(\alpha) \cdots q_s(\alpha)$$
$q_1(\alpha), \ldots q_s(\alpha) \neq 0 \Rightarrow (\alpha - \alpha_j)^{m_j} = 0$ for some $j$
$\Rightarrow \alpha = \alpha_j$ for some $j$.
Now: $\deg p = m_1 + \cdots + m_k + \sum_{j=1}^{s} \deg q_j \geq m_1 + \cdots + m_k$
and $m_1 + \cdots + m_k$ is the # of roots of $p(x)$ counted with multiplicities. $\square$

## Back to groups

**Recall** A group is a set $G$ together with two operations
$G \times G \to G$, $(a,b) \mapsto ab$ "multiplication"
$G \to G$, $a \mapsto a^{-1}$ "inversion"
and an element $e \in G$ so that

(i) $g \cdot e = g = e \cdot g$ for all $g \in G$

(ii) $g \cdot g^{-1} = e = g^{-1} \cdot g$ —//—

(iii) $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ for all $g_1, g_2, g_3 \in G$

ie. multiplication is associative

**Remarks**

(1) Identities are unique: suppose $\exists e' \in G$ s.t. $ge' = g = e'g$ for all $g \in G$. Then $e = ee'$.
But $e$ is an identity. Hence $ee' = e'$. $\therefore e = e'$

(2) Inverses are unique: fix $a \in G$. Suppose $\exists b \in G$ s.t. $ab = e = ba$.
Then $b = b \cdot e = b \cdot (a \cdot a^{-1}) = (ba)a^{-1} = e a^{-1} = a^{-1}$.

**Definition** Let $(G, \circ, e)$ be a group (with $^{-1}: G \to G$ understood).
A subgroup of $G$ is a nonempty subset $H$ of $G$ such that

1) $e \in H$

2) $\forall h_1, h_2 \in H$, $\underset{\text{mult. in } G}{h_1 \circ h_2} \in H$

3) $\forall h \in H$, $h^{-1} \in H$.

**Remarks** • $(H, \circ, e)$ is a group in its own right.

• $(2) + (3) \Rightarrow (1)$. Reason: Since $H \neq \emptyset$, $\exists h \in H$.
By (3) $h^{-1} \in H$. By (2) $e = h \cdot h^{-1} \in H$.

**Notation** $H < G$ if $H$ is a subgroup of $G$.

**Ex** $(\mathbb{Z}, +, 0)$ is a subgroup of $(\mathbb{R}, +, 0)$

$\mathbb{N} \cup \{0\} = \{n \in \mathbb{Z} \mid n \geq 0\}$ is not a subgroup of $(\mathbb{Z}, +, 0)$.