Thm [Division algorithm]

① If $f, g \in K[x]$, $g \neq 0$, then $\exists\, q, r \in K[x]$ such that $f = gq + r$, with $r = 0$ <u>OR</u> $0 \leq \deg r < \deg g$.

② If f, g have no common constant factors, $\exists$ polynomials r, s such that $fr + gs = 1$.

③ If $p \in K[x]$ is irreducible and $p \mid fg$ then $p \mid f$ or $p \mid g$

④ Every non-zero polynomial f can be written as $f = c p_1 \cdots p_r$ with c a unit and p_i irreducible polynomials. This is unique upto reordering and multiplication by units.

① Follows from "long division" (Thm 23.1)

② Is the Euclidean algorithm of polynomials

④ I prove in class assuming ③.

Ex.
- x^2+1 is irreducible in $\mathbb{R}[x]$
- $x^3+x+1 = (x+1)(x^2-x+2) - 1$
- $x+1$ is a factor of x^3+1

Defn
- Let $f \in K[x]$. An element $\alpha \in K[x]$ is called a <u>root / zero of f</u> if $f(\alpha) = 0$ in K.
- If $K' \supseteq K$ is a larger field and $\alpha \in K'$

satisfies $f(\alpha)=0$, then we say α is a root of f in K'. (In general we can evaluate polynomials in larger fields)

(Of course α is a root $\iff f \in \ker ev_\alpha$, where $ev_\alpha : K[x] \to K, f(x) \mapsto f(\alpha)$)

Ex i is a root of x^2+1 in $\mathbb{C}$, not in $\mathbb{R}$.

Prop Let $f \in K[x]$. Then f has a root in K $\iff$ f has a linear factor

Pf If $f(x) = (x-c)g(x)$ for $c \in K$, $g(x) \in K[x]$ then $f(c) = (c-c)g(c) = 0$
$\Rightarrow f$ has a root in K.

Conversely, $f \in \ker ev_\alpha$ for some $\alpha \in K$.
Apply division algorithm to f and $x-\alpha$
i.e. $f(x) = (x-\alpha)q + r$ with $r=0$ or $\deg r < \deg(x-\alpha) = 1$. Thus r is a constant.
But $0 = f(\alpha) = (\alpha-\alpha)q + r = r$
$\Rightarrow r = 0$
$\Rightarrow f(x) = (x-\alpha)q$
$\Rightarrow f$ has a linear factor ∎

Cor Let $f(x) \in K(x)$ be a polynomial of degree $n \geq 0$. Then it has at most n distinct roots

Pf If α_1 is a zero of $f(x)$, then
$f(x) = (x-\alpha_1)\, g_1(x)$ and $\deg g_1(x) = n-1$
If α_2 is a zero of $g_1(x)$ we have $f(x) = (x-\alpha_1)(x-\alpha_2)\, g_2(x)$.
Proceeding in this way we obtain,
$f(x) = (x-\alpha_1)\cdots(x-\alpha_r)\, g_r(x)$ with g_r having no zeroes in K.
Since $\deg f = n \Rightarrow r \leq n$. Moreover, if
$f(b) = 0 \Rightarrow (b-\alpha_1)\cdots(b-\alpha_r)\, g_r(b) = 0$
$\Rightarrow b - \alpha_i = 0$ for some i as $g_r(b) \neq 0$ and K is a domain
$\Rightarrow \alpha_1, \ldots, \alpha_r$ are all the zeros of f ∎

Cor If $f, g \in K[x]$ of degree n and f, g agree for atleast $n+1$ values in K, then $f = g$.

Cor Let K be an infinite field. Let $f, g \in K[x]$ s.t. $F(\alpha) = g(\alpha)$ $\forall\, \alpha \in K$. Then $f = g$.

Exercise Show $f(x) = x^p - x \in (\mathbb{Z}/p\mathbb{Z})[x]$ is zero for every value of $\mathbb{Z}/p\mathbb{Z}$.

Conclusion Polynomials SHOULD NOT be thought of as functions