Thm. If D is a UFD, so is $D[x]$.

Proof: Let $f \in D[x]$ of deg n. Then

- f is a prod. of finitely many polys of deg ≥ 1.

Thus, we only need to prove irr. $\equiv$ prime.

Suppose f is irr. and $f \mid gh$. Then $f(x) q(x) = g(x) h(x)$ for some $q(x) \in D[x]$.

If $\deg f = 0$, then: $f(x) = a \in D$ irreducible, $a \cdot c(q(x)) = c(g(x)) \cdot c(h(x)) \Rightarrow a \mid c(g(x)) \cdot c(h(x))$.

As D is a UFD, $a \mid g(x)$ or $a \mid h(x)$. i.e. $f(x)$ is a prime.

If $\deg f = n > 0$, Let K be the fraction field of D. Then $f(x)$ is irreducible in $K[x]$.

and so f is prime, since K is a field and $K[x]$ is an ED.

Thus, $f \mid g$ or $f \mid h$. WLOG, let $f \mid g$. i.e. $g(x) = f(x) \cdot d(x)$ for some $d(x) \in K[x]$. ($d(x) \notin D[x]$)

Let r be the prod. of the denominators of the coefficients of $d(x)$.

Then $r g(x) = f(x) \cdot (r d(x))$ in $D[x]$. let $a = c(r \cdot g(x))$ and $b = c(f(x) \cdot r \cdot d(x)) = c(r \cdot d(x))$.

$r \cdot g(x) = a \cdot g_1(x)$. $r \cdot d(x) = b \cdot d_1(x)$.

Then $a g_1(x) = b f(x) d_1(x)$ where $g_1(x)$, $f(x)$, $d_1(x)$ are primitive by Gauss lemma.

So $a = bu$ with u inv. and $u g_1(x) = f(x) d_1(x)$, and $f(x) \mid g_1(x)$, $f(x) \mid g(x)$. i.e. f is prime in $D[x]$. $\square$

Let F be a field.

$D = F[x]$, $I = (f(x))$. then $D/I = F[x]/(f(x))$ is a field if $f(x)$ is irr.

Field Theory

Let F be a field. finite: $\mathbb{F}_p$, $\mathbb{F}_4$.

infinite: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Let F be a field. Let n be the smallest positive integer s.t. $n \cdot 1 \equiv 0$. (If such n doesn't exist, define $\mathrm{char}(F) = 0$).
Then n is called the <u>characteristic</u> of F. denoted $\mathrm{char}(F)$

If $F < E$, then F is a <u>subfield</u> of E, E is an <u>extension</u> of F.

<u>eg</u>. $F = \mathbb{Q}$, $E = \mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{-1}]$, $\mathbb{R}$, $\mathbb{C}$.

Let $F < E$.

Def. Let $S \subset E$, and let $F(S)$ be the intesection of all subfields of E which contain F and S. Then $F(S)$ is a field, and extension field of F. (eg. $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[2] = \mathbb{Q}$)

In particular, if $S = \{\alpha\}$, then $F(S) = F(\alpha)$.

Def. α is called an <u>algebraic elt</u> (代数元.) over F if $f(\alpha) = 0$ for some $f(x) \in F[x]$.

otherwise, α is called a <u>transcendental elt.</u> (超越数.) say π.

Prop. Let $F < E$, and $\alpha \in E \setminus F$.

(1) If α is transcendental, then $F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \,\middle|\, f, g \in F[x],\ g \neq 0 \right\}$.

(2) If α is algebraic, then $F(\alpha) \cong F[x] / (m(x))$, where $m(x)$ is s.t. $m(\alpha) = 0$ and $m(x) \mid f(x)$, if $f(\alpha) = 0$

$\qquad$ ||| $m(x)$ irr.

$\quad$ $m(x)$ is irreducible

$\quad$ |||

$\quad$ $m(x)$ is a minimal poly s.t. $m(\alpha) = 0$.

Proof: Let $\alpha : F[x] \longrightarrow F(\alpha)$
$$\frac{f(x)}{g(x)} \longmapsto \frac{f(\alpha)}{g(\alpha)}$$

Then α is a ring homo with $\ker \alpha = \{ f(x) \in F[x] \mid f(\alpha) = 0 \}$

If α is transcendental, then $\ker \alpha = \{0\}$.

If α is algebraic, then $\ker \alpha = (m(x))$.

$\mathbb{F}_9 > \mathbb{F}_3$. $\quad$ $\mathbb{F}_3[x]$. x^2+1 irreducible. $\qquad$ x^2+1 $\qquad$ x^2+x+2

$$\mathbb{F}_3[x] / (x^2+1) \cong \mathbb{F}_9.$$

HW: $\mathbb{F}_3[x]/(x^2+1) \overset{?}{\cong} \mathbb{F}_3[x]/(x^2+x+2)$

$$\| $$
$$(\{0, 1, -1, x, -x, x+1, x-1, -x+1, -x-1\}, \oplus, \otimes).$$

$\mathbb{F}_{p^2} > \mathbb{F}_p$. $\quad x^2 - r \quad \exists\, r \in \mathbb{F}_p$. $\quad x^2 - r$ irreducible

$$\mathbb{F}_{p^2} \cong \mathbb{F}_p[x] / (x^2 - r) = (\{ ax+b \mid a, b \in \mathbb{F}_p \}, \oplus, \otimes).$$

Thm. For any $n \in \mathbb{Z}^+$, there exist irreducible poly of deg n in $\mathbb{F}_p[x]$.

Proof: $n = 2$.

There are exactly p^2 polys with the form $a + bx + x^2$.

Among them, reducible ones are either $(a_0+x)(a_0+x)$, or $(a_0+x)(b_0+x)$ with $a \neq b$.

$$\underbrace{p}_{\#} + \underbrace{\frac{p(p-1)}{2}}_{\#} = \frac{1}{2}p(p+1) < p^2.$$