Factorization in $\mathbb{Z}[x]$

$\mathbb{Z}$ PID. but $\mathbb{Z}[x]$ is not.

$$\mathbb{Z}[x] \hookrightarrow \underbrace{\mathbb{Q}[x]}_{\text{PID}}$$

Goal: $\mathbb{Z}[x]$ is UFD.

Typical problem:

$R \hookrightarrow R'$. R is a subring of R'.

If $r \in R$ is irreducible in R, r may not be irreducible in R'.

Ex: $R = \mathbb{R}[x]$. $R' = \mathbb{C}[x]$.

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

We use two constructions to analyse $\mathbb{Z}[x]$

$\mathbb{Z}[x] \hookrightarrow \mathbb{Q}[x]$, $\varphi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ p prime

Defn. (Primitive polynomial).

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0.$$

① $a_n > 0$, $n \geq 1$

② $g.c.d(a_n, \dots a_0) = 1$.

Ex: $f(x) = 2x^2 + 2x + 3$.

Non. Ex: $f(x) = 2x^2 + 4x + 6$.

Lemma: ① $p \mid a_i$

② $p \mid f$

③ $\varphi_p(f) = 0$

① $\Leftrightarrow$ ② $\Leftrightarrow$ ③

Lemma: ① f primitive

equivalent ② $\forall p$ prime number. $p \nmid f$

① $\Leftrightarrow$ ② $\Leftrightarrow$ ③ ③ $\varphi_p(f) \neq 0$ for all p prime number

Lemma: p prime element in $\mathbb{Z}[x]$ iff p prime element in $\mathbb{Z}$.

Pf: $\mathbb{Z}[x]/(p) = \mathbb{F}_p[x]$

$\mathbb{F}_p$ is integral domain $\Leftrightarrow$ $\mathbb{F}_p[x]$ is integral domain

(Gauss lemma). $f, g \in \mathbb{Z}[x]$ are both primitive $\Leftrightarrow$ $f \cdot g$ is primitive

Pf: $\forall p$, $\varphi_p(f \cdot g) = \varphi_p(f) \cdot \varphi_p(g)$.

and $\mathbb{F}_p[x]$ has no zero divisors

so $\varphi_p(f \cdot g) \neq 0 \Leftrightarrow \varphi_p(f) \neq 0, \varphi_p(g) \neq 0$

(It's quit hard to prove directly!)

$f(x) \cdot g(x)$ the coefficient for

x^3 is $\underline{a_1 b_2 + a_2 b_1 + a_3 b_0 + a_0 b_3}$.

It's hard to figure out the prime factors for the sum of products).

Lemma: $\forall f \in \mathbb{Q}[x] \Rightarrow f = c \cdot f_0(x)$

$c \in \mathbb{Q}$, $f_0(x) \in \mathbb{Z}[x]$ and primitive.

c, f_0 are uniquely determined by f

(If $f(x) \in \mathbb{Z}[x]$, then $c \in \mathbb{Z}$)

Pf: Existence:

$$f(x) = \frac{2}{3}x^2 + \frac{4}{5}x + 6$$

$$\Rightarrow f(x) = \frac{1}{15}(10x^2 + 12x + 90)$$

$$= \frac{\frac{2}{15}}{C} \frac{(5x^2+6x+x_5-)}{f_0(x)}.$$

uniqueness: If

$$f(x) = C_0 f_0 = C_0' f_0'.$$

then $mf(x) = (C_0 m) f_0$

$$= (C_0' m) f_0'.$$

choose m such that

$$C_0 m, \quad C_0' m \in \mathbb{Z}$$

For $p \mid C_0 m \Rightarrow p \mid mf(x)$

$$\Rightarrow p \mid (C_0' m) f_0'$$

$\Rightarrow \; p \mid c_0' m$ (since f_0 is primitive)

Cancel p on both sides.

$\Rightarrow \; c_0 m = c_0' m$ use induction

$\Rightarrow \; f_0(x) = f_0'(x)$.

Thm: (1) f_0 primitive in $\mathbb{Z}[x]$

$g \in \mathbb{Z}[x]$

If $f_0 \mid g$ in $\mathbb{Q}[x]$

then $f_0 \mid g$ in $\mathbb{Z}[x]$

Pf. Assume $g = f_0 \cdot h$.

$h(x) \in \mathbb{Q}[x]$.

$h(x) = c\, h_0(x)$. $c \in \mathbb{Q}$, $h_0(x) \in \mathbb{Z}[x]$ primitive

$g = c' g_0(x)$

$g = c' g_0(x) = c\,(\underbrace{f_0 \cdot h_0}_{})$

Gauss Lemma $\Rightarrow f_0 h_0$ primitive.

Uniqueness $\Rightarrow c = c' \in \mathbb{Z}$ (since $g(x) \in \mathbb{Z}[x]$)

So $h(x) \in \mathbb{Z}[x]$.

(2) If f, g has common divisor in $\mathbb{Q}[x]$.

then f, g has common divisor in $\mathbb{Z}[x]$.

Pf: $h \mid f$. then $h_0 \mid f$.

Thm: $f(x)$ irreducible in $\mathbb{Z}[x]$ $a_n > 0$.

then $f(x) =$ prime number in $\mathbb{Z}$

or primitive irreducible in $\mathbb{Q}[x]$.

pf: $\deg f = 0. \Rightarrow f$ is is $\mathbb{Z}$.

f prime in $\mathbb{Z} \Leftrightarrow f$ prime in $\mathbb{Z}[x]$.

If $f(x)$ is primitive polynomial in $\mathbb{Z}[x]$.

then
$$\boxed{\begin{array}{l} g(x) \mid f(x) \text{ in } \mathbb{Q}[x] \\ \Leftrightarrow g_0(x) \mid f(x) \text{ in } \mathbb{Z}[x] \quad (*) \end{array}}$$

Thm: Every irreducible element in $\mathbb{Z}[x]$ is a prime element.

Pf: Prove it for primitive polynomials

Use $(*)$ again.

(Division in $\mathbb{Z}[x]$ is the same in $\mathbb{Q}[x]$ when considering primitive polynomials.)

Thm: $\mathbb{Z}[x]$ is UFD.

$$f(x) = c \cdot f_0(x)$$

$$c = p_1 \cdots p_m$$

$$f_0(x) = g_1 \cdots g_k(x)$$

$g_i(x)$ primitive, irreducible in $\mathbb{Q}[x]$

Thm: If R is UFD, then $R[x]$ is UFD.

(same proof)

Ex: $\mathbb{C}[x][y] = \mathbb{C}[x,y]$. (UFD but not PID)

Why care $\mathbb{Z}[x]$.

Consider field extension for $\mathbb{Q}$.

Is $\mathbb{Q}[x]/(f(x))$ a field?

Want to know whether $f(x)$ irreducible in $\mathbb{Q}[x]$.

It's equivalent to $f_0(x)$ irreducible in $\mathbb{Z}[x]$.

In $\mathbb{Z}[x]$, we can consider

$\varphi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x]$

and use correspondance theorem.

Next class : Eisenstein Criterion.