

Factorisation in $\mathbb{Z}[x]$ vs $\mathbb{Q}[x]$

~~irred in $\mathbb{Z}[x]$~~ does not factor into poly. of lower deg.

R a ring $r \in R$ is reducible if it has a non-trivial factorisation.

$$r = s \cdot t \quad s, t \in R \text{ neither a unit.}$$

Irreducible = not ~~is~~ reducible.
= no non-trivial factorisation.

$$\begin{aligned} 3x^2 + 3 &\in \mathbb{Z}[x] \text{ is } \underline{\text{reducible}} \\ &= 3 \cdot (x^2 + 1) \\ &\in \mathbb{Q}[x] \text{ is } \underline{\text{irreducible.}} \end{aligned}$$

Def: $f(x) \in \mathbb{Z}[x]$ is primitive if no prime p divides all the coeff.

Ex. $x^3 + 27$ primitive, $2x^2 + 4x + 3$ primitive

Thm: Let $f(x) \in \mathbb{Z}[x]$ be primitive polynomial.
Then $f(x)$ is reducible in $\mathbb{Z}[x]$ iff
reducible in $\mathbb{Q}[x]$.

Obs: 1) Any $f(x) \in \mathbb{Z}[x]$ can be written as
 $d \cdot g(x)$ $d \in \mathbb{Z}$, $g(x) \in \mathbb{Z}[x]$ primitive.
unique up to sign. = unique upto units of \mathbb{Z} .

2) Any $f(x) \in \mathbb{Q}[x]$ can be written as
 $f(x) = d \cdot g(x)$, $d \in \mathbb{Q}$, $g(x) \in \mathbb{Z}[x]$ primitive.
unique up to sign.

$$\begin{aligned}
\frac{1}{2}x^2 + \frac{2}{3}x &= \frac{1}{6} \cdot (3x^2 + 4x) \\
&= \frac{1}{12} (6x^2 + 8x) \\
&= \left(\frac{1}{12} \cdot 2 \right) \cdot \underline{(3x^2 + 4)}
\end{aligned}$$

Lemma (Gauss) : — Let $f(x), g(x) \in \mathbb{Z}[x]$ be primitive.

Then $f(x)g(x)$ is primitive.

Pf: ~~Take~~ Take a prime p . Look at

$$\mathbb{Z}[x] \rightarrow \mathbb{Z}/p\mathbb{Z}[x]$$

$$f(x) \mapsto \overline{f(x)} \quad \text{non-zero}$$

$$g(x) \mapsto \overline{g(x)} \quad \text{non-zero}$$

$$f(x)g(x) \mapsto \overline{f(x)} \cdot \overline{g(x)} \quad \text{non-zero}$$

□.

Pf of Thm: $f(x)$ red. in $\mathbb{Z}[x] \Rightarrow f(x)$ reducible in $\mathbb{Q}[x]$.
(easy).

$f(x)$ red in $\mathbb{Q}[x]$. want $f(x)$ red. in $\mathbb{Z}[x]$.

$$f(x) = g(x) \cdot h(x), \quad g(x), h(x) \in \mathbb{Q}[x]$$

Write $g(x) = r_1 \cdot g_1(x)$ $r_1 \in \mathbb{Q}$ $g_1(x) \in \mathbb{Z}[x]$ prim.
 $h(x) = r_2 \cdot h_1(x)$ $r_2 \in \mathbb{Q}$ $h_1(x) \in \mathbb{Z}[x]$ prim.

$$1 \cdot \underbrace{f(x)}_{\text{prim.}} = (r_1 r_2) \underbrace{(g_1(x) \cdot h_1(x))}_{\text{prim.}} \quad \text{so } r_1 r_2 = \pm 1$$

$$f(x) = \pm g_1(x) \cdot h_1(x), \quad h_1, g_1 \in \mathbb{Z}[x].$$

□

$$\underline{\mathbb{Z}}[x]$$

vs

$$\mathbb{Q}[x]$$

$$\underline{\mathbb{C}}[t][x]$$

vs

$$\underline{\mathbb{C}(t)}[x]$$

$$\underline{F[t]}[x]$$

vs

$$\underline{F(t)}[x]$$

, F field.

$$P_0(t) + P_1(t)x + \dots + P_n(t)x^n$$

$$P_i \in F[t]$$

primitive if no irred. poly in $F[t]$ divides all. $P_i(t)$.

For prim. elt of $F[t][x]$, red. in

$$F[t][x] = \text{red. in } F(t)[x].$$

$$R[x]$$

vs.

$$(\text{fr. field } R)[x]$$

R has unique factorisation.

Ex: $x^3 + x^2 - t \in \mathbb{Q}(t)[x]$ is irreducible.

$x^3 + x^2 - t \in \mathbb{Q}[t][x]$ primitive.

~~$t \nmid x^3 + x^2$~~

$$\mathbb{Q}[t, x]$$

$$\mathbb{Q}[x, t]$$

$x^3 + x^2 - t \in \mathbb{Q}[x][t]$ primitive

$$x^3 + x^2 - t \in \mathbb{Q}(x)[t]$$

\hookrightarrow irred. (deg 1).