Examples

- Observe that x^2-5 is irreducible in $\mathbb{Q}[x]$ but is not irreducible in $\mathbb{R}[x]$.

$$x^2-5=(x+\sqrt{5})(x-\sqrt{5})$$

[Since both $\mathbb{Q}$ & $\mathbb{R}$ are UFD's, there does not exist any other factorization of x^2-5 in $\mathbb{R}$ unless we have one factor is $u(x+\sqrt{5})$, where u is a unit in $\mathbb{R}[x]$.

— The units in $\mathbb{R}[x]$ are the nonzero constants.]

- Observe that x^2+1 is irreducible in $\mathbb{Z}_3[x]$ but not in $\mathbb{Z}_5[x]$.

<u>Note:</u> In $\mathbb{Z}_5[x]$, $x^2+1=(x-2)(x-3)$. ✓

Why is this not possible in $\mathbb{Z}_3[x]$?

$$(x-1)(x-1)=x^2-2x+1=x^2+x+1$$
$$(x-1)(x-2)=x^2+2$$
$$(x-2)(x-2)=x^2+2x+1 \qquad -4\equiv 2 \bmod 3$$

$(x-0)$ doesn't work

so x^2+1 is irreducible in $\mathbb{Z}_3[x]$.

Facts about $R[x]$, where R is an ID. ← integral domain.

- ($p(x)\in R[x]$ and $p(x)=(x-a)q(x)$ for some $q(x)\in R[x]$) $\iff p(a)=0$ (in R)

- $\mathbb{Z}[x]$.
  - A polynomial $p(x)\in\mathbb{Z}[x]$ factors in $\mathbb{Q}[x]$ $\iff$ $p(x)$ factors in $\mathbb{Z}[x]$.

[Idea of proof: Assume a complete factorization in $\mathbb{Q}[x]$, keep track of denominators → multiply through & show we can change to polynomials with integer coefficients.]

○ Mod p Irreducibility test.

If $f(x) \in \mathbb{Z}[x]$ reduces in $\mathbb{Z}[x]$, then it also reduces in $\mathbb{Z}_p[x]$ for any prime p.

○ Eisenstein Criterion Let

$$f(x) = a_0 + a_1 x + \dots + a_k x^k \in \mathbb{Z}[x]$$

Suppose that for some prime p, $p \nmid a_k$, $p \mid a_j$ for all $j < k$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ (or $\mathbb{Q}[x]$).

Example: prove that $x^6 - 75x^2 - 9x + 300$ is irreducible in $\mathbb{Q}[x]$.

Proof: For prime $p = 3$, the E. Criterion is satisfied, so it's irreducible.

Fact: In any integral domain, if $\underbrace{a \in (R \setminus \{0\}) \setminus R^\times}_{\text{a is nonzero \& not a unit}}$ is prime, then a is irreducible.

Proof: Sp. $a \in (R \setminus \{0\}) \setminus R^\times$ is prime, and suppose $a = bc$. Because a is prime, $a \mid b$ or $a \mid c$. WLOG, say $a \mid c \Rightarrow c = ra$ for some $r \in R \Rightarrow a = bra \Rightarrow (1 - br)a = 0$

$\therefore 1 - br = 0 \Rightarrow br = 1 \Rightarrow b$ is a unit.

$\Rightarrow a$ is irreducible. $\boxtimes$

<u>Thm</u> In a PID, R, an element $p \in R$ is prime $\Leftrightarrow$ $p \in R$ is irreducible.

<u>Proof</u>: Suppose $p \in R$, a PID, and p is irreducible.
then $\langle p \rangle$ is maximal $\Rightarrow$ $\langle p \rangle$ is prime.
Sp. $p \mid a \cdot b$ with $a, b \in R$. Then
$ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle \Leftrightarrow p \mid a$ or $p \mid b$. $\blacksquare$

A commutative ring R satisfies the ACC (ascending chain condition) if whenever a sequence of ideals $I_1, I_2, \ldots$ satisfies

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots,$$

then there exists $k \in \mathbb{N}$, such that

$$I_{k+a} = I_k \quad \text{for all } a \in \mathbb{N}.$$

<u>Defn</u> A <u>Noetherian Ring</u> is a commutative ring that satisfies the ACC.
