

Recall:

Thm $R[x]$ is a UFD iff R is a UFD.Key ideas

1. $R \hookrightarrow$ Field of fractions F so
 $R[x] \hookrightarrow F[x]$, $F[x]$ a UFD
2. Let $p(x) \in R[x]$ where R is a UFD, let $d = \gcd(\text{coefs})$.
 Then $p(x) = d \cdot p'(x)$ where
 p' irred in $R[x] \rightarrow$ irred in $F[x]$.
3. Factors over $F \xrightarrow[\text{clearing}]{\text{denom}}$ Factors over R

Question Suppose R an I.D. and $p(x) \in R[x]$ is monic, irreducible.
 Must $p(x)$ be irred. in $F[x]$?

Answer No!Example

$$R = \mathbb{Z}[i] \quad F = \mathbb{Q}[i]$$

$$p(x) = x^2 + 1 \text{ irred in } R[x]$$

$$\hookrightarrow = (x+i)(x-i) \text{ in } F[x]$$

COR $\mathbb{Z}[i]$ is not a UFD

(Proven last term)

Some irreducibility Tests

Prop Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$.

Suppose $\frac{r}{s} \in \mathbb{Q}$ in lowest terms, $p(\frac{r}{s}) = 0$. Then
 $r|a_0, s|a_n$

In particular if $p(x)$ is monic then the only possible roots are divisors of a_0 .

Proof $a_n (\frac{r}{s})^n + a_{n-1} (\frac{r}{s})^{n-1} + \dots + a_0 = 0$

$$a_n r^n + a_{n-1} s r^{n-1} + \dots + a_0 s^n = 0$$

$$\left. \begin{aligned} a_n r^n &= -s(a_{n-1} r^{n-1} + \dots + a_0 s^{n-1}) && \text{Thus } s|a_n \\ a_0 s^n &= -r(\dots) && r|a_0 \quad // \end{aligned} \right\}$$

Examples

1. $x^3 + 2x^2 - 2$ is irreducible in $\mathbb{Z}[x]$.

Proof If it factors over \mathbb{Z} it factors over \mathbb{Q} , thus it has a rational root thus it is $\pm 1, \pm 2$ but none are.

2. $x^2 \pm p, x^3 \pm p$ irreducible for p prime.

Remark This technique does not work for large degree polynomials.

Remark Notice that the proof works for any UFD and its field of fractions.

Prop Let $I \subset R$ an integral domain, $p(x)$ monic in $R[x]$.
 If $\bar{p}(x) \in (R/I)[x]$ does not factor into 2 polys
 of smaller degree, then $p(x)$ is irreducible.

Proof Suppose not, so $p(x) = a(x)b(x)$ in $R[x]$. Observe that
 wlog both are monic so $\bar{p} = \bar{a}\bar{b}$.

Example 1

$p(x) = x^3 + 7x + 5 \in \mathbb{Z}[x]$, reduce mod 2
 $\bar{p}(x) = x^3 + x + 1$ is irred, so $p(x)$ is

Example 2

$x^4 + 1$ irred in $\mathbb{Z}[x]$ but reducible mod any prime
 $x^4 - 7ax^2 + 4$ irred in $\mathbb{Z}[x]$ but reducible mod every integer!

Famous Special Case:

Eisenstein Criterion

Let $P \subset R$ prime ideal, R an int dom.

$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$. Suppose

$$a_{n-1}, \dots, a_1, a_0 \in P$$

$$a_0 \notin P^2$$

Then $f(x)$ is irreducible in $R[x]$

Proof

Suppose not so $f(x) = a(x)b(x)$ reduce mod P

$$x^n = \bar{a}(x)\bar{b}(x)$$

Now R/P is an integral domain so both $\bar{a}(x)$ & $\bar{b}(x)$ have zero const term

Thus $a_0 \in P^2$ ✗

Example $x^5 + 14x^3 + 49x + 21$ is irred in $\mathbb{Z}[x]$. (thus in $\mathbb{Q}[x]$)

Example $x^n - p$ irred $\forall n$, thus $\sqrt[n]{p}$ is irrational.

Example Let $f(x) = x^4 + 1$ if $f(x)$ factors, so does $f(x+1)$.

But $f(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$ irred $p=2$.

Example $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1$ cyclotomic polynomial.

$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + p x^{p-2} + \dots + \binom{p}{2} x + p$ irred

Thus $\Phi_p(x)$ is irreducible.

Some "random" results.

Prop Max ideals in FCS are $(f(x))$ / f irred.

Proof In a PID prime \leftrightarrow maximal.

More generally...

Prop Factor $f(x) = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ into irred.

$$FCS/(f(x)) \cong \prod_{i=1}^s FCS/(p_i)^{a_i}$$

Proof $(p_i^{a_i}) + (p_j^{a_j})$ are comaximal

Prop #roots of a degree n poly is $\leq n$ (counted w/mult)

Proof Induce + UFD

Cor Let F be a field, $G \leq F^*$, $|G| < \infty$.
Then G is cyclic.

Proof $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$
with $n_1 | n_2 | \dots | n_k | n$

Thus each $\mathbb{Z}/n_i\mathbb{Z}$ has at least n_i elts of order n_i

Thus $x^{n_i} - 1$ has too many roots.

Corollary $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ distinct primes.

1. $(\mathbb{Z}/n\mathbb{Z})^{\times} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^{\times} \times \dots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^{\times}$

2. $(\mathbb{Z}/2^{\alpha}\mathbb{Z})^{\times} \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$

3. $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{\times} \cong \mathbb{Z}_{p^{\alpha-1}(p-1)}$ p odd

Remark Thus we know $\text{Aut}(\mathbb{Z}/n)$