What are...irreducible polynomials?

Or: Analogs of primes

What is special about prime numbers?

What we know is:

$\mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow$ n is prime

What we want to have is:

$\mathbb{K}[X]/(f)$ is a field $\Leftrightarrow$ f is irreducible

- $\mathbb{Q}[X]/(X^2-2) \cong \mathbb{Q}(\sqrt{2})$, the isomorphism is $X \mapsto \sqrt{2}$ Field
- $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$, the isomorphism is $X \mapsto i$ Field
- In $\mathbb{Z}[X]/(X^2)$ the polynomial X is not invertible Not a field

Prime are irreducible

Multiplication table of $\mathbb{Z}/4\mathbb{Z}$

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- In $\mathbb{Z}$ is 4 reducible $4 = 2 \cdot 2$
- Thus, $2 \cdot 2 = 0$ in $\mathbb{Z}/4\mathbb{Z}$
- We have $4\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$
- With contrast, for $n = 2$ we have

$$(a \cdot b = 2) \text{ implies } (a = 2 \text{ or } b = 2 \text{ up to units})$$

and $\mathbb{Z}/2\mathbb{Z}$ is a maximal ideal

Zero divisors and $0 = 1$

Zero divisors can not be invertible:

$$(a \cdot b = 0 \text{ and } b \cdot c = 1) \text{ implies } (0 = 1)$$

- In $\mathbb{R}[X]$ is $X^2 - 2$ reducible $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$
- Thus, $(X - \sqrt{2})(X + \sqrt{2}) = 0$ in $\mathbb{R}[X]/(X^2 - 2)$
- We have *e.g.* $(X^2 - 2) \subset (X - \sqrt{2}) \subset \mathbb{R}[X]$
- With contrast, in $\mathbb{Q}[X]$ we have

$$(a \cdot b = X^2 - 2) \text{ implies } (a = X^2 - 2 \text{ or } b = X^2 - 2 \text{ up to units})$$

and $(X^2 - 2)$ is a maximal ideal

For completeness: The formal definition

A polynomial $f \in R[X_1, ..., X_n]$ is irreducible if

$$(a \cdot b = f) \Rightarrow (a = f \text{ or } b = f \text{ up to units})$$

- We have
$$\mathbb{K}[X]/(f) \text{ is a field} \Leftrightarrow f \text{ is irreducible}$$
- Irreducible polynomials are primes in polynomials
- Being irreducible depends on the underlying ring
- Figuring out whether f is irreducible is key

Examples.

- Irreducible $\Rightarrow$ no roots in R; the converse is false
- $(f \in \mathbb{C}[X] \text{ is irreducible}) \Leftrightarrow (f \text{ is of degree one})$
- $(f \in \mathbb{R}[X] \text{ is irreducible}) \Leftrightarrow (f$ is of degree one or $f = (X - a)(X - b)$ for a, b not real$)$

The rich world of field extensions of $\mathbb{Q}$

Theorem (Eisenstein)

For p prime, take a polynomial $f = a_n \cdot X^n + ... + a_0 \in \mathbb{Z}[X]$ that satisfies:

(a) p divides $a_0, ..., a_{n-1}$

(b) p does not divide a_n

(c) p^2 does not divide a_0

Then f is irreducible in $\mathbb{Q}[X]$

- This applies to infinitely many polynomials of arbitrary degree, *e.g.*

$$X^n + p \cdot (X_{n-1} + ... + 1)$$

- Any cyclotomic polynomial is irreducible

$$f(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + ... + 1$$

because we can substitute

$$f(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{p-1} X^{p-2} + ... + \binom{p}{1}$$

Thank you for your attention!

I hope that was of some help.