Recall:

A field is a ring where every nonzero element is invertible.

Example $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ are all fields.

Next goal: Use fields to construct other interesting rings that let us shed light on the integers.

If $\mathbb{K}$ is any field. (\mathbb(K).)

Can form the polynomial ring $\underline{\mathbb{K}[x]}$.

the set of all polynomials in the variable x with coefficients in $\mathbb{K}$

Multiply and add them in the obvious way.

Interesting fact: $\mathbb{K}[x]$ is a lot like $\mathbb{Z}$.

Example: There is unique factorization in $\mathbb{K}[x]$.

Notion of prime polynomials, gcds, etc.

Eg. on $\mathbb{R}[x]$ x^2+1 is a prime polynomial.

$x^2+1 = 2\left(\frac{1}{2}x^2 + \frac{1}{2}\right)$.

not divisible by a non-constant polynomial of smaller degree.

Today: Euclidean algorithm in $\mathbb{K}[x]$.

Just like Euclidean algorithm in $\mathbb{Z}$.

$\longrightarrow$ If $a(x)$ $b(x)$ $\in \mathbb{K}[x]$

then it computes $\gcd(a(x), b(x))$

and if you unfold gives

$$a(x)s(x) + b(x)t(x) = \gcd(a(x), b(x))$$

$\gcd(a(x), b(x))$ — the largest degree monic polynomial that divides both $a(x)$ and $b(x)$

monic: $x^n + c_{n-1}x^{n-1} + \cdots + c_0$.

leading coefficient is 1.

Ex. 4 - (1)

$$
\begin{array}{r|l}
 & x^2 - 2x + 4 \\
3x+1 & 3x^3 - 5x^2 + 10x - 3 \\
- & 3x^3 + x^2 \\
= & \quad -6x^2 + 10x - 3 \\
- & \quad -6x^2 - 2x \\
= & \quad\quad 12x - 3
\end{array}
$$

$$
\begin{aligned}
- \quad & 12x + 4 \\
= \quad & -7
\end{aligned}
$$

So $$\underbrace{3x^3 - 5x^2 + 10x - 3}_{a(x)} = \underbrace{(x^2 - 2x + 4)}_{q(x)}\underbrace{(3x+1)}_{b(x)} + \underbrace{-7}_{r(x)}$$

---

4. After doing 4-(3) try to also find the prime factorizations of

$$x^3 + x^2 + 1 \quad \text{and} \quad x^3 + x^2 \quad \text{in } \mathbb{Z}/3\mathbb{Z}[x].$$

and compute the gcd by comparing them.

This is written

as $\mathbb{F}_3[x]$

on unrotated.