

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

Can form the polynomial ring $K[x]$.

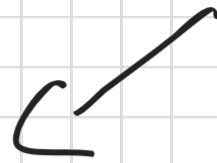
the set of all polynomials in the variable x with coefficients in K

Multiply and add them in the obvious way.

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

Example: There is unique factorization in $K[x]$.
Notion of prime polynomials, gcds, etc.

Eg. in $\mathbb{R}[x]$ 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 $K[x]$.

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

→ If $a(x)$ $b(x) \in K[x]$

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: $x^n + c_{n-1}x^{n-1} + \dots + c_0$.
 leading coefficient is 1.

Ex. 4 - (1)

$$\begin{array}{r}
 x^3 - 2x + 4 \\
 \hline
 3x + 1 \overline{) 3x^3 - 5x^2 + 10x - 3} \\
 \underline{-(3x^3 + x^2)} \\
 -6x^2 + 10x - 3 \\
 \underline{-(6x^2 + 2x)} \\
 -8x - 3 \\
 \underline{-(8x + 8)} \\
 5
 \end{array}$$

$$= \frac{12x + 4}{-7}$$

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

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

$$x^3 + x^2 + 1 \quad \text{and} \quad x^3 + x^2 \text{ in } \mathbb{F}_{32}[x].$$

and compute the gcd by comparing them.

This is written
as $f_3(x)$
on worksheet.

