Finite fields

1) F field: commutative ring with unity s.t. every $x \neq 0$ is invertible.

Ex: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/_p = \mathbb{F}_p$ for every prime p.

Field $\Rightarrow$ integral domains

$$xy = 0 \Rightarrow x = 0 \text{ or } y = 0$$

Fields are good becaus

① linear algebra is possible

speak about vector spaces on a field

② $F[x]$ polynomial ring over F

$\hookrightarrow$ very nice structure.

- Division algorithm: given $f, g \in F[x]$, $g \neq 0$

  $\exists!\ q, r \in F[x]$

  $$f = gq + r \qquad r = 0 \text{ or } \deg(r) < \deg(f).$$

- $\exists \ \underbrace{\gcd(f,g)}_{d}$ for every $f, g \in F[x]$

  unique up to multiplication by $\lambda \in F^*$.

- $F[x]$ PID $\Rightarrow$ UFD
- Euclide algorithm.
- Bézout identity

  $$\gcd(f,g) = A f + B g \qquad A, B \in F[x].$$

- $f \in F[x]$ has at most n roots in F where $n = \deg f$.

F field $f \in F[x]$

$\leadsto$ quotient ring $F[x]/f = A$ $\deg f = n$

each element in A can be represented uniquely as a polynomial of degree $< n$

$\hookrightarrow$ A vector space on F of dimension n

$\bar{g}$ class of g in A

$\bar{g} = \bar{r}$ where r is the remainder of the division of g by f.

- if f irreducible then

$A = F[x]/f$ is a field.

+ F- vector space

and $F \subseteq A$ F subfield of A

or A extension of F.

$x \in A$ $a_0 + a_1 X + a_2 X^2 + \dots + a_{n-1} X^{n-1}$

If F is finite then

$|A| = |F|^n \Rightarrow A$ is finite.

in particular in $F = \mathbb{F}_p$ then $|A| = p^n$

every finite extension of $\mathbb{F}_p$ has order p^n some n.

Conversely, every finite field K must contain $\mathbb{F}_p$ for some p.

$1 \in \mathbb{F}_p$ consider the additive order of 1.

↳ characteristic of K

"char (K)"

smallest $m > 0$ s.t. $m 1 = 0$ in K

m must be prime: indeed if $m = rs$

then $0 = m \cdot 1 = (r \cdot 1)(s \cdot 1)$ ⇝ one of

$(r \cdot 1) = 0$ or $(s \cdot 1) = 0$

⇝ $r \cdot 1 = 0$ or $s \cdot 1 = 0$ $\Rightarrow$ $r = 0$ or $s = 0$.

$\Rightarrow$ Finite fields have a prime char. p

⇝ they contain a copy of $\mathbb{F}_p$

$0, 1, 2 \cdot 1, \ldots, (p-1) \cdot 1$

⇝ every finite field has order p^t some t.

Example

$p = 3$ $\quad \mathbb{F}_3 = \{0, 1, 2\}$

$f = x^3 + x^2 + x + 2 \in \mathbb{F}_3[x]$ $\quad n = 3$

$f(0) = 2 \quad f(1) = 2 \quad f(2) = 1$ $\quad$ no roots in $\mathbb{F}_3$

↳ irreducible $(\deg = 3)$

$$K = \frac{\mathbb{F}_3[x]}{f} = \{ aX^2 + bX + c \mid a, b, c \in \mathbb{F}_3 \}$$

Operations :

- sum

$$(2 + x + x^2) + (1 + 2x) = \underbrace{(2+1)}_{=3=0} + \underbrace{(1+2)}_{3=0} x + x^2 = x^2$$

- $(2 + x + x^2) \cdot (1 + 2x) = 2x^3 + 2x + 2$ mod f

$$= x^2 + 1$$

remainder by the division by f.

$$2x^3 + 2x + 2 \;\Big|\; \underline{x^3 + x^2 + x + 2}$$

$$\cdot\, 2$$

$$\overline{\quad x^2 + 1 \quad}$$

- Inverse of a pol. g in K.

↳ very similar to the case $\mathbb{Z}_m$

Assume for ex to compute

$(1 + 2x)^{-1}$ in K

Since f is irreducible

$\gcd(1 + 2x, f(x)) = 1$

Compute Bézout identity

$$x^3 + x^2 + x + 2 = (2x+1)(2x^2+x) + 2$$
$$2x+1 = 2(x+2) + 0$$

Bézout : $2 = x^3+x^2+x+2 - (2x+1)(2x^2+x)$ in $\mathbb{F}_3[x]$

Multiply by $2^{-1} = 2$

$$1 = 2f - 2(2x+1)(2x^2+x)$$

modulo f (in K)

$$1 = (2x+1)\cdot \underbrace{(-2)(2x^2+x)}_{= \, 2x^2+x}$$

$$(2x+1)^{-1} = 2x^2+x \quad \text{in } \mathbb{F}_3[x]$$

---

① $\forall p, \forall n$ $\exists$ an irreducible f in $\mathbb{F}_p[x]$

$\rightsquigarrow$ $\exists K$ s.t. $|K| = p^n$

② All fields of order p^n are <u>isomorphic</u>

If $q = p^n$ we call

$\mathbb{F}_q$ <u>the</u> (unique) field with q elements.