Question: Classify all finite fields.

(*) Want: a finite field

$\mathbb{F}$ of $\operatorname{char}\mathbb{F} = p$

must have $\#\mathbb{F} = p^n$

for some n.

Saw $\mathbb{F}$ is a vector space / $\mathbb{F}_p$

$\Rightarrow$ $\mathbb{F} \cong \mathbb{F}_p^n$

Proposition: Let $\mathbb{F}$ be a finite field of $\operatorname{char}\mathbb{F} = p$. Then $(\mathbb{F}, +, 0)$ is isomorphic to

$\underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}$ for some n.

n-times

Proof: By classification of finite abelian gps,

(*) $(F, +, 0) \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{\alpha_k}}$

for (not nec. distinct) primes $p_1, \ldots, p_k$ w/ $\alpha_1, \ldots, \alpha_k \geq 1$.

If for some i, $p_i \neq p$, then by Cauchy there is an element of order p_i, but the additive order of each $x \in F$ is p

$$p \cdot x = 0$$

(if $n \cdot x = 0$ then

$$\underbrace{(1 + \cdots + 1)}_{n\text{- times}} \cdot x = 0 \Big)$$

So $p_1 = \cdots = p_k = p$

If for some i, $\alpha_i > 1$,

Then $\mathbb{Z}_{p_i^{\alpha_i}} \subseteq \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{\alpha_k}}$

and by the converse of Lagrange theorem for finite abelian gps, there is $x \in \mathbb{F}$ of order

$$o(x) = p_i^{\alpha_i} = p^{\alpha_i}$$

in contradiction to the fact that $o(x) = p$.

Thus $\alpha_1 = \cdots = \alpha_k = 1$

$$(\mathbb{F}, +, \cdot) \cong \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$$

So $(F, +, \cdot)$ $\underbrace{\quad\quad\quad\quad\quad\quad\quad\quad}_{n\text{- times}}$

for some n. //

Cor: In this case

$$\#F = p^n.$$

Next: Understanding the mult. table.

Def: Let F be a field.

A polynomial over F is a formal expression

$$f(x) = \overbrace{a_n x^n}^{\text{monomial}} + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

where $\forall i$, $a_i \in F$.

We denote

$F[x]$ = set of all

polynomials

+ 0 polynomial

The degree of f is n

if $a_n \neq 0$ and n is the maximul index such that $a_n \neq 0$.

$\deg(0) = -\infty$ by convention.

- Two polynomials / $\mathbb{F}$

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \begin{pmatrix} a_i \in \mathbb{F} \\ b_i \in \mathbb{F} \end{pmatrix}$$

$$g(x) = \sum_{i=0}^{m} b_i x^i$$

are equal if

$n = m$ and $\forall \; 0 \leq i \leq n$

$a_i = b_i$ (in F)

Observe: every polynomial

$f(x) \in F[x]$ defines

a function

$$\hat{f} : F \longrightarrow F$$

$$a \longmapsto f(a)$$

eg: say $F = F_2 = \{0, 1\}$

$f(x) = x^2$, $g(x) = x$

$f \neq g$ but (in / out)

$\hat{f} = \hat{g} : F_2 \longrightarrow F_2$

as functions

$0 \longmapsto 0$

$1 \longmapsto 1$

Opin

$\sum_{i=0}^{n}$

If $\begin{cases} f(x) = \sum_{i=0}^{n} a_i x^i \\ g(x) = \sum_{i=0}^{m} b_i x^i \end{cases}$

w/o g, say $m \le n$.

- $f(x) + g(x) = \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i$

ie $\deg(f+g) = \max\{\deg f, \deg g\}$

- $f(x) \cdot g(x) = \left(\sum_{j=0}^{n} a_j x^j\right)\left(\sum_{j=0}^{m} b_j x^j\right)$

$$= \sum_{k=0}^{n+m} c_k x^k$$

$$i+j=k$$

$$c_k = \sum_{\substack{i=0,\dots,n \\ j=0,\dots,m}} a_j b_{i-j}$$

$$\left(a_n x^n + a_{n-1} x^{n-1} + \dots + a_0\right)\left(b_m x^m + \dots + b_0\right)$$

$$a_n b_m x^{n+m} + \left(a_{n-1} \cdot b_m x^{n+m-1} + a_n b_{m-1} x^{n+m-1}\right) + \dots$$

$$= a_n b_m x^{n+m} + \underbrace{\left(a_{n-1} b_m + a_n b_{m-1}\right)}_{c_{n+m-1}} x^{n+m-1} + \dots$$

Ex: $F = \mathbb{F}_2$ $\quad f(x) = x^2 + x - 1$

$$g(x) = x + 1$$

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

$$= x^3 + x^2 + x^2 + x - x - 1$$

$= x^3 + 2x^2 + x - x - 1 = x^3 + 2x^2 - 1$

$= x^3 - 1$

- Let $f(x) \in \mathbb{F}[x]$ and $t \in \mathbb{F}$.

  Then t is called a zero/root of f if

  $$f(t) = 0$$

$\mathbb{F}[x] \subseteq \mathbb{K}[x]$

Rem: If $\mathbb{F} \subseteq \mathbb{K}$ a subfield inclusion then $f(x) \in \mathbb{F}[x]$ also $f(x) \in \mathbb{K}[x]$

eg: $f(x) = x^2 + 1$, $\mathbb{F} = \mathbb{R}$

then f has no zeros

for $f(x) \in \mathbb{C}[x]$

$i \in \mathbb{C}$ is a zero of f.

We defined

$$+ : F[x] \times F[x] \longrightarrow F[x]$$

$$\cdot : F[x] \times F[x] \longrightarrow F[x]$$

associative op'n.

0 is neutral wrt "+"

1 is neutral wrt "·"

$-f(x)$ is the additive inverse to $f(x)$

- $f(x) \in F[x]$ has mult. inverse iff $\deg f = 0$

  ie $f(x) = c$, $c \neq 0 \in F$:

  if $g(x) \in F[x]$ satisfy

$$f(x)\,g(x) = 1$$

then

$$\deg f + \deg g = \deg(f \cdot g) = \deg(1) = 0$$

$$\Rightarrow \deg f = 0 \wedge \deg g = 0$$

So $\mathbb{F}[x]$ is "almost" a field.

<u>Long division</u> / Euclidean algo.

Slogan: polynomials (in one variable) are analogous to integers.

Let $\mathbb{F}$ be a field

and $n \geq m$

$(\deg f = n)$ $\{ \; f(x) = \underline{a_n} x^n + \cdots + a_1 x + a_0$

$(\deg g = m) \mid g(x) = b_m x^m + \cdots + b_1 x + b_0$

w/ $m \le n$ $\quad a_n, b_m \neq 0.$

Set $n_0 = n$, $c_0 = \frac{a_n}{b_m}$

$r_0(x) = f(x) - c_0 x^{n_0 - m} \cdot g(x) = r_1(x)$

$a_n x^n \quad \left(\frac{a_n}{b_m} \cdot x^{n-m} \cdot b_m \cdot x^m + \cdots\right)$

$= (a_{n-1} - b_{m-1} c_0) \cdot x^{n-1}$

$+ \cdots$

So $n_1 = \deg r_1 < \deg f = n_0$

If $n_1 < m = \deg(g)$

we are done, otherwise

$\to r_1(x) - c_1 \cdot x^{n_1 - m} \cdot g(x) = r_2(x)$

Where $n_2 = \deg r_2 < \deg r_1 = n_1$

and we continue until

$$n_i < m.$$

At the end we get:

$$r_0(x) = f(x) = c_0 x^{n_0 - m} \cdot g(x) + r_1(x)$$

$$r_1(x) = c_1 x^{n_1 - m} g(x) + r_2(x)$$

$$\vdots$$

$$\rightarrow \quad r_{s-1}(x) = c_{s-1} x^{n_{s-1} - m} g(x) + r_s(x)$$

$$f(x) = g(x) \cdot \underbrace{\left(c_0 x^{n_0 - m} + \dots + c_{s-1} x^{n_{s-1} - m} \right)}_{q(x)} + \underbrace{r_s(x)}_{r(x)}$$

w/ $\deg r_s < \deg g = m.$

Thus $f \,\%\, g = r$ quotient

$$f(x) = g(x)\,q(x) + r(x).$$

remainder.

Thm: For $f, g \in \mathbb{F}[x]$

w/ $\deg f \geq \deg g$ $\exists$ unique

poly's $q, r \in \mathbb{F}[x]$ s.t.h

$$(*)\quad f(x) = g(x)\,q(x) + r(x).$$

Proof: Suppose also $q'(x), r'(x)$

satisfy

$$(**)\quad f(x) = g(x)\,q'(x) + r'(x)$$

Then

$$g(x)\,q(x) - r'(x) = g(x)\,q'(x) - r(x)$$

$(\rightleftharpoons)$

$$(***)\quad g(x)\left(q(x) - q'(x)\right) = r(x) - r'(x)$$

by design, $\deg r, \deg r' < \deg g$

so $\deg(r - r') < \deg(g)$

since

$$\deg(g \cdot (q - q')) =$$

$$\deg g + \deg(q - q')$$

we must have

$$q = q'$$

from which it follows that $r(x) = r'(x)$. //

Cor: If $f(x) \in F[x]$

and $a \in F$ is a root

of f then

$$f(x) = (x-a) \cdot f'(x)$$

for some $f'(x) \in F[x]$

Proof: do long division of

$f(x)$ by $g(x) = (x-a)$.

so $\exists\ q, r \in F[x]$ s.t.

$$f(x) = (x-a)\,q(x) + r(x).$$

substituting a:

$$0 = f(a) = (a-a)\,g(a) + r(a)$$

so $r(a) = 0$.

But $\deg r < \deg (x-a) = 1$

hence

$$r = 0.$$

$\Rightarrow$ $f(x) = (x-a) \cdot q(x)$. //

Cor: A polynomial of degree n over $\mathbb{F}$ can have at most n roots.

Proof: If $f(x) \in \mathbb{F}[x]$, $\deg f = n$ w/ $m > n$ distinct roots, $a_1, \dots, a_m$ then

$f(x) = (x - a_1) q_1(x)$

a_2 is a root of $q_1(x)$

$q_1(x) = (x - a_2) q_2(x)$

$$f(x) = \prod_{i=1}^{m} (x - a_i) \cdot q(x)$$

- contradicting the assumption $m > n$. //

$$\gcd(f, g) = \gcd\begin{pmatrix} (x-1)\cdot(x+2) \\ (x-1)\cdot(x^2+2) \end{pmatrix} = x - 1$$

"Elementary number theory"