Theorem

Every finite field has order p^r for some prime number p and positive integer r.

Proof: If $\mathbb{F}$ is a finite field with n elements

then we can consider

$S = \{ m \cdot 1 : m \in \mathbb{Z} \}$ is a subring.

$$m \cdot 1 = \begin{cases} \underbrace{1+1+\cdots+1}_{m} & \text{if } m \in \mathbb{N} \\ 0 & \text{if } m = 0 \\ \underbrace{(-1)+\cdots+(-1)}_{(-m)} & \text{if } -m \in \mathbb{N} \end{cases}$$

has order p, which is a prime.

Otherwise. $|S| = ab$

$$\Rightarrow \underbrace{(1+\cdots+1)}_{a}\underbrace{(1+\cdots+1)}_{b} = (ab)\cdot 1 = 0$$

View $\mathbb{F}$ as a vector space over $S \cong \mathbb{Z}_p$

under addition: $(\mathbb{F}, +)$ is a group

$x, y \in \mathbb{F}$

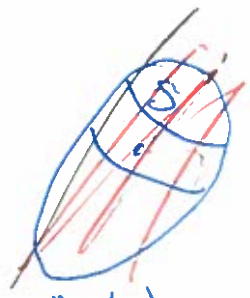
$(m\cdot 1)(x+y) = (m\cdot 1)x + (m\cdot 1)y$

$1 \cdot x = x$

$(m\cdot 1)(n\cdot 1)x = \cdots$

$\exists$ a basis $B = \{v_1, \cdots v_r\}$ of $\mathbb{F}$ over S.

$a_i \in S$.



$(\mathbb{R}^n, +)$

$\forall \lambda x \in \mathbb{R}^n \quad \lambda \in \mathbb{R}, x \in \mathbb{R}^n$

$\lambda(x+y) = \lambda x + \lambda y$.

$(\lambda\mu)x = \cdots$

Theorem Every polynomial $f(x) \in F[x]$ has a solution in $E = F[x]/\langle g(x) \rangle$ for some $g(x)$ that divides $f(x)$.

Example $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. has no zero in $\mathbb{Q}$

First: note that ~~there is no~~ $f(x)$ is irreducible.

If not $(x^2-2) = (x-a)(x-b)$ $a, b \in \mathbb{Q}$

~~$(x^2-2) = (x-a)(x-b)$, $a, b \in \mathbb{Q}$~~

~~But then $ab = -2$!!!~~

~~$a+b$~~

then by factor theorem.

$f(a) = 0$, i.e. $a^2 - 2 = 0$, $a \in \mathbb{Q}$!!!

$(x-a)$

$f(x) = g(x)q(x) + r(x)$

$A = \langle x^2-2 \rangle = \{ (x^2-2) g(x) : g(x) \in \mathbb{Q}[x] \}$

$\mathbb{Q}[x]/A = \{ ax+b+A : a, b \in \mathbb{Q} \}$.

$(ax+b+A) + (cx+d+A) = (a+c)x + (b+d) + A$.

$(ax+b+A)(cx+d+A) =$

$= acx^2 + (bc+ad)x + bd + A$

$= ac(x^2-2) + 2ac + (bc+ad)x + bd + A$

$= (bc+ad)x + (bd+2ac) + A$

Let $\alpha = x + A \in \mathbb{E} = \mathbb{Q}[x]/A$

identify $q \in \mathbb{Q}$ with $q + A$. So that $\mathbb{Q} \subseteq \mathbb{E}$.

$\alpha^2 - 2$

$= (x+A)^2 - (2+A)$

$= (x^2-2) + A = 0 + A = \underline{0}$

Also observe that $\mathbb{E} \cong \{ a\sqrt{2} + b : a, b \in \mathbb{Q} \}$

Example $f(x) = x^2+1 \in \mathbb{Q}[x]$

$f(x) = x^2+1$ is irreducible. $f(a) \neq 0 \ \forall a \in \mathbb{Q}$

$\mathbb{E} = \mathbb{Q}[x]/A \qquad A = \langle x^2+1 \rangle = \{(x^2+1)g(x) : g(x) \in \mathbb{Q}[x]\}$

$= \{ax+b+A : a,b \in \mathbb{Q}\}$.

$(ax+b+A) + (cx+d+A) = (a+c)x + (b+d) + A$

$(ax+b+A)(cx+d+A)$

$= acx^2 + (ad+bc)x + bd + A$

$= ac(x^2+1) - ac + (ad+bc)x + bd + A$

$= (ad+bc)x + (bd-ac) + A$

In $\mathbb{E}$, let $\alpha = x+A$,

$\alpha^2 + 1$

$= (x+A)(x+A) + (1+A)$

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

Identify $q+A$ as $q \in \mathbb{Q}$ so that $\mathbb{Q} \subseteq \mathbb{E}$

Example: $\mathbb{Z}_2[x]$.

$f(x) = x^3 + x + 1$

has no zero in $\mathbb{Z}_2$.

If it does, $f(a) = 0$ for $a \in \mathbb{Z}_2$.

$f(0) = 1 \neq 0$

~~$f(1) = 1 \neq 0$~~

Moreover $f(x)$ is irreducible

If it is, then $f(x) = g(x)\,h(x)$.

$= (x-a)(x^2 + bx + c)$

$\Rightarrow$ ~~$(x-a)$~~ a is zero !!!

Consider $A = \langle x^2 + x + 1 \rangle = \{(x^3+x+1)g(x) : g(x) \in \mathbb{Z}_2[x]\}$

Then $F = \mathbb{Z}_2[x]/A = \{ ax^2 + bx + c : a, b, c \in \mathbb{Z}_2 \}$

$+A$

$(a_1x^2 + b_1x + c_1) + (a_2x^2 + b_2x + c_2) = (a_1+a_2)x^2 + (b_1+b_2)x + c_1 + c_2 + A$

$+A \qquad +A$

$(a_1x^2 + b_1x + c_1)(a_2x^2 + b_2x + c_2) = a_1a_2x^4 + (a_1b_2 + a_2b_1)x^3 + (a_1c_2 + b_1b_2 + c_1a_2)x^2 + (\quad)x + (c_1c_2) + A$

$+A \qquad +A$

$(x^3 + x + 1)a_1a_2x - (a_1a_2x^2 + a_1a_2x)$

$+ \quad -$

(1) $\alpha = x + A$ satisfies

$\alpha^3 + \alpha + 1$

$= (x+A)^3 + (x+A) + (1+A)$

$= (x^3 + x + 1) + A = 0 + A = 0$ ✓

$a + A$ is identified with $a \in \mathbb{Z}_2$

$\therefore \mathbb{Z}_2 \subseteq \mathbb{F}$

$(\mathbb{F}^*, \cdot) \cong (\mathbb{Z}_7, +)$

$\therefore$ $\exists$ θ

In $(\mathbb{F}^*, \cdot)$, except $1+A$, every element is a generator

$x^3 + x + 1 = 0$

$x + A$

$(x+A)^2 = x^2 + A$

$(x+A)^3 = x^3 + A = (-x-1) + A = x + 1 + A$

$(x+A)^4 = (x+1+A)(x+A) = x^2 + x + A$

$(x+A)^5 = (x^2 + x + A)(x+A) = x^3 + x^2 + A = x + 1 + x^2 + A$

$(x+A)^6 = (x+1+x^2+A)(x+A) = x^3 + x^2 + x + A = (x+1)(x^2+x) + A$

$= x^2 + 1 + A$

$(x+A)^7 = (x^2+1+A)(x+A) = x^3 + x + A = 1 + A$ //

$(x+A)^{-1} = (x^2 + 1 + A)$