Positive Integers
Before Humanity
Some animals can count

Group?
closed under $+$
$\times$

0
How can nothing be something

Positive Rational
Group? $(\mathbb{Q}^+, \times)$ is a group.
$(\mathbb{Q}, +, \times)$ Field
$(\mathbb{R}, +, \times)$ Field
$(\mathbb{C}, +, \times)$ $a+bi$

Field F is a group under $+$
and $F - \{0\}$ is a group under $\times$
If F_1 & F_2 are fields and $F_1 \subseteq F_2$
How do they relate?

Def W is a vector over over a field F
$(W, F, +, \cdot)$
$(W, +)$ is a group
$\cdot : F \times W \to W$ (scalar Mult)
$\lambda(\alpha v) = (\lambda\alpha) v$
$\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$

1. $V = V$

$\mathbb{Q} \subseteq \mathbb{R}$ $\quad [\mathbb{R} : \mathbb{Q}]$ is uncountable

$\mathbb{R} \subseteq \mathbb{C}$ $\quad \mathbb{C} = a + bi$

Where did $\mathbb{C}$ come from? $\mathbb{R}$?

Question. Does $\exists$ a field F s.t. $\mathbb{Q} \subset F \subset \mathbb{R}$

$a, b, c, d \in \mathbb{Q}$

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$$

$$(a+c) + (b+d)\sqrt{2}$$

$a + b\sqrt{2} \neq 0$

$a = -b\sqrt{2}$

$\sqrt{2} = \frac{a}{b}$

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$$

$$ac + (ad+bc)\sqrt{2} + 2bd = (ac+2bd) + (ad+bc)\sqrt{2}$$

Field?

$$a+b\sqrt{2}\left(\frac{a-b\sqrt{2}}{a^2-2b^2}\right) = \frac{a^2-2b^2}{a^2-2b^2} = 1$$

$a^2 - 2b^2 = 0 \quad = \frac{a^2}{b^2} = 2 \quad \frac{a}{b} = \sqrt{2}$

$a + b\sqrt{3} \qquad a + b\sqrt{3}$

$a + b\sqrt[3]{2} + c\sqrt[3]{4}$ $\qquad q = \sqrt[3]{2}$

$a + bq + cq^2 = a + 2q + 2q^2 + 2q^3 + 2q^4$

$2q^3 = 2q$

$(a + bq + cq^2)(d + eq + fq^2)$

$= 1$

$a+bi \qquad \mathbb{R}[x] \qquad x^2+1$

$$I = \{f(x)(x^2+1) \mid f(x) \in \mathbb{R}[x]\}$$

$(I, +)$ a group? $\qquad R$

$(I,+)$ a group?

Is $(I,\times)$ closed

What are cosets of $\frac{R}{I}$?

$\frac{R}{I}$

$f(x) = g(x)(x^2+1)+r$

$\deg(r) \le 1$

all cosets look like $(ax+b)I$

$(cx+d)I$

$\frac{acx^2+(bc+ad)x+bd}{x^2+1} = g(x)(x^2+1)+r$

$acx^2+(bc+ad)x+bd\,(I)$

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

$(ax+b)I\,(cx+d)I = (bd-ac)+(ad+bc)x$

$a+bi$

$c+di$

$(ac-bd)+(ad+bc)i$

$\frac{\mathbb{Q}[x]}{(x^3-2)}$

$\frac{\mathbb{Q}[x]}{(x^2-2)}$

Poly must be irreducible

$\mathbb{R} \subset F \subset \mathbb{C}$

Finite $|F|$ finite. Look

$1, 1+1, 1+1+1, \cdots$

$1, 2, 3, \cdots n = 0$

What about n?

n has to be prime else zero divisors!

Prime subfield. (1) $2 \times a = a+a$

$n \times a = a+a+\cdots$

$\mathbb{Z}_p \subseteq \mathbb{F}$ $\dim \frac{\mathbb{F}_2}{\mathbb{Z}_p}$ finite

$\beta \in \mathbb{F} - \mathbb{Z}_p$ $a+b\beta$ $a, b \in \mathbb{Z}_p$

$a+b\beta = c+d\beta$ $(a-c) = (d-b)\beta$

if $d-b \neq 0$ $\beta = \frac{a-c}{d-b} \in \mathbb{Z}_p$ impl.

$\mathbb{F}_2$ $\{a+b\beta \mid a,b \in \mathbb{Z}_p\}$ has p^2

$\gamma \in \mathbb{F} - \mathbb{F}_2$ $a+b\beta+c\gamma$ all lin ind

$a_0 + a_1\beta_1 + a_2\beta_2 + \cdots a_{k-1}\beta_{k-1}$ dim k

p^k

$\forall$ finite fields $|\mathbb{F}|$ $\exists$ prime p $|\mathbb{F}| = p^k$ for some k

$\mathbb{Z}_2$ x^2+1 is not irred

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

Master Theorem

a) $\forall p^k$, $\exists$ a finite field $\mathbb{F}$ s.t. $|\mathbb{F}| = p^k$

b) any two finite fields of the same size are iso

c) In a finite field $\mathbb{F}$, $(\mathbb{F} - \{0\}, \times)$ is a cyclic group of order $p^k - 1$

$\exists$ generator g

d) Elts of $\mathbb{F}$ satisfy $x^q - x = 0$ $q = p^k$

$x(x^{q-1} - 1)$

$x(x^{q^n-1}-1)$

~~2)~~

~~3)~~ A field of order p^k contains a field of order p^d iff $d \mid k$ (d divides)

~~4)~~ Every irred poly of deg r in $\mathbb{F}_p[x]$ is a factor of $x^q - x$ when $q = p^r$