



Fields

Book III

We have been talking about number fields: finite extensions $E \supseteq \mathbb{Q}$ i.e. $[E:\mathbb{Q}] = n < \infty$.
(Some are Galois i.e. $G = \text{Aut } E$ satisfies $|G| = n$; but in general $|G| \leq n$.)

Back to basics:

In a field F , if $\underbrace{1+1+\dots+1}_{n \geq 1} = 0$ then the smallest n for which this occurs is the characteristic of F .

If F has characteristic $n > 0$ then n must be prime. If $n = ab$, $a, b \geq 1$ then

$$\underbrace{(1+1+\dots+1)}_a \underbrace{(1+1+\dots+1)}_b = \underbrace{1+1+\dots+1}_{n=ab} = 0$$

By minimality of n , n is prime.

If $\underbrace{1+1+\dots+1}_n \neq 0$ for any $n \geq 1$, then we say n has characteristic 0.

Given a field F , $\text{char } F =$ characteristic of F is either 0 or p (some prime p).

• If $\text{char } F = p$ then $F \supseteq \mathbb{F}_p =$ field of order p ($\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\} =$ "integers mod p ").

eg. $\mathbb{F}_p, \mathbb{F}_{p^2}, \mathbb{F}_{p^3}, \mathbb{F}_{p^4}, \dots, \mathbb{F}_p(x) = \{ \text{all rational functions in } x \text{ with coefficients in } \mathbb{F}_p \}, \dots$

• If $\text{char } F = 0$ then $F \supseteq \mathbb{Q}$. Eg. $\mathbb{R}, \mathbb{C}, \mathbb{Q}$, number fields, $A = \{ \text{algebraic numbers} \} \subset \mathbb{C}$
eg. $\mathbb{Q}[\sqrt{2}]$

In either case F has a unique smallest subfield, either \mathbb{F}_p or \mathbb{Q} , called the prime subfield of F .

All fields of characteristic 0 are infinite. (They are extensions of \mathbb{Q} , hence vector spaces over \mathbb{Q} .)

If $E \supseteq F$ is a field extension (i.e. E, F are fields with F a subfield of E) then E is a vector space over F . The dimension of this vector space is the degree $[E:F]$ of this extension eg.

$$[\mathbb{C}:\mathbb{R}] = 2$$

$\{1, i\}$ basis

$$[\mathbb{R}:\mathbb{Q}] = \infty$$

$1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{10}, \sqrt{11}, \dots$
are lin. indep.

$$[\mathbb{C}:\mathbb{Q}] = \underbrace{[\mathbb{C}:\mathbb{R}]}_2 \underbrace{[\mathbb{R}:\mathbb{Q}]}_{\infty} = \infty$$

For fields of characteristic a prime p , some are finite, some are infinite.

Given p prime and $k \geq 1$ (positive integer), there is a unique field of order $q = p^k$ (up to isomorphism)

Finite fields: $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_8, \mathbb{F}_9, \mathbb{F}_{11}, \mathbb{F}_{13}, \mathbb{F}_{16}, \mathbb{F}_{17}, \dots$

$$\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$$

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$$\alpha + \alpha = (1+1)\alpha = 0\alpha = 0$$

\times	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

$$\text{char } \mathbb{F}_4 = 2.$$

$\mathbb{F}_4 \supset \mathbb{F}_2$ of degree $[\mathbb{F}_4:\mathbb{F}_2] = 2$

with basis $1, \alpha$

$$\begin{aligned} \mathbb{F}_4 &= \{a \cdot 1 + b\alpha : a, b \in \mathbb{F}_2\} \\ &= \{0, 1, \alpha, 1+\alpha\} \quad \text{where } \alpha^2 = \alpha+1. \\ &= \{0, 1, \alpha, \alpha^2\} \quad \beta \end{aligned}$$

$$\mathbb{F}_4 = \mathbb{F}_2[\alpha]$$

The minimal poly. of α over \mathbb{F}_2 is $x^2 + x + 1$.

Irreducible polynomials over $\mathbb{F}_2 = \{0, 1\}$

degree 1: $x, x+1$ (both irreducible)

degree 2: $x^2, x^2+1, x^2+x, x^2+x+1$
 $\underbrace{x \cdot x \quad (x+1)(x+1) \quad x(x+1)}_{\text{reducible}}$ irreducible

degree 3: $x^3 = x \cdot x \cdot x$
 $x^3+1 = (x+1)(x^2+x+1)$
 $x^3+x = x \cdot (x+1)^2$
 x^3+x+1 irreducible
 $x^3+x^2 = x \cdot x \cdot (x+1)$
 x^3+x^2+1 irreducible
 $x^3+x^2+x = x(x^2+x+1)$
 $x^3+x^2+x+1 = (x+1)^3$

There are 2ⁿ polynomials of degree n: $x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$
 and they are all monic. $c_0, c_1, \dots, c_{n-1} \in \mathbb{F}_2$

Let α be a root of x^2+x+1 . The other root is $\alpha+1$.

$$\alpha^2 + \alpha + 1 = 0 \Rightarrow \alpha^2 = -\alpha - 1 = \alpha + 1$$

Note: The roots of $ax^2+bx+c=0$ are $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$
 except in characteristic 2.

$\mathbb{F}_8 = \mathbb{F}_2[\gamma]$ where γ is a root of x^3+x+1
 $= \{a + b\gamma + c\gamma^2 : a, b, c \in \mathbb{F}_2\}$
 $= \{0, 1, \gamma, \gamma+1, \gamma^2, \gamma^2+1, \gamma^2+\gamma, \gamma^2+\gamma+1\}$
 $\quad \quad \quad \underbrace{\quad}_{\gamma^3} \quad \quad \quad \underbrace{\quad}_{\gamma^6} \quad \quad \quad \underbrace{\quad}_{\gamma^4} \quad \quad \quad \underbrace{\quad}_{\gamma^5}$

ie. $\gamma^3 = \gamma + 1$

$\gamma^0 = 1$

$\gamma^1 = \gamma$

$\gamma^2 = \gamma^2$

$\gamma^3 = \gamma + 1$

$\gamma^4 = \gamma^2 + \gamma$

$\gamma^5 = \gamma^3 + \gamma^2 = \gamma^2 + \gamma + 1$

$\gamma^6 = \gamma^3 + \gamma^2 + \gamma = (\gamma + 1) + \gamma^2 + \gamma$

$= \gamma^2 + 1$

$\gamma^7 = \gamma^3 + \gamma = (\gamma + 1) + \gamma = 1$

x^3+x+1 has three roots in \mathbb{F}_8 :
 $\gamma, \gamma^2, \gamma^4$

x^3+x^2+1 has three roots in \mathbb{F}_8 :
 $\gamma^3, \gamma^5, \gamma^6 = \gamma^7$

In general the nonzero elements of \mathbb{F}_q
 form a cyclic group of order $q-1$.

There is only one finite field of each order $q=p^k$
 (p prime, $k \geq 1$) up to isomorphism.

If \mathbb{F}_q is a finite field then it must have $\text{char } \mathbb{F}_q = p$ for some prime p

$|\mathbb{F}_q| = q < \infty$

So \mathbb{F}_q is an extension $\mathbb{F}_q \supseteq \mathbb{F}_p$ hence a vector space of some dimension k .

Let $\alpha_1, \dots, \alpha_k$ be a basis for \mathbb{F}_q over \mathbb{F}_p ie. $\mathbb{F}_q = \{q_1\alpha_1 + q_2\alpha_2 + \dots + q_k\alpha_k : q_1, \dots, q_k \in \mathbb{F}_p\}$

$q = |\mathbb{F}_q| = p^k$

$$\mathbb{F}_9 = \mathbb{F}_3[i] \quad \text{compare: } \mathbb{C} = \mathbb{R}[i],$$

$$= \{a+bi : a, b \in \mathbb{F}_3\}$$

$$= \{0, 1, 2, i, 1+i, 2i, 1+2i, 2+2i\}$$

$$\begin{matrix} \theta^0 & \theta^1 & \theta^2 & \theta^3 & \theta^4 & \theta^5 & \theta^6 & \theta^7 & \theta^8 \end{matrix}$$

θ is a primitive element: its powers give all the nonzero elements of \mathbb{F}_9 .

$$\mathbb{Q}[i] \supset \mathbb{Q}, \quad i = \sqrt{-1}$$

$$\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$$

$\{1, i\}$ is a basis of the extension in each case.

$$i = \sqrt{-1} = \sqrt{2} \quad \mathbb{F}_9 = \mathbb{F}_3[i] = \mathbb{F}_3[\sqrt{2}]$$

$$\theta^0 = 1$$

$$\theta^1 = \theta = 1+i$$

$$\theta^2 = (1+i)^2 = 1+2i+i^2 = 2i$$

$$\theta^3 = \frac{2i(1+i)}{\theta^2 \theta} = -2+2i = 1+2i$$

$$\theta^4 = \theta^2 \theta = (1+2i)(1+i) = 1-2 = -1 = 2$$

$$\theta^5 = \theta^4 \theta = -\theta = 2\theta = 2+2i$$

$$\theta^6 = \theta^4 \theta^2 = -\theta^2$$

$$\theta^7 = \theta^4 \theta^3 = -\theta^3$$

$$\theta^8 = \theta^4 \theta^4 = -\theta^4$$

Every finite field \mathbb{F}_q ($q = p^k$, p prime)

has a primitive element i.e. an element whose powers give all the nonzero field elements.

Why? Idea of proof: Eg. to see that \mathbb{F}_9 has a primitive element: The nonzero elements form a multiplicative group of order 8. There are five groups of order 8 up to isomorphism:

- dihedral group of order 8 (symmetry group of a square) } nonabelian
- quaternion " " " " }

abelian

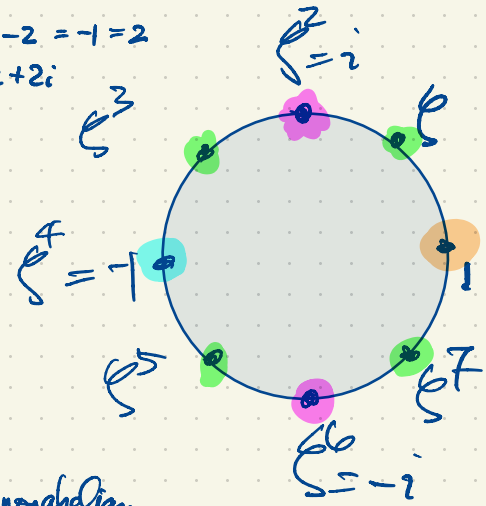
- C_8 (four elements of order 8, one element of order 2)
- $C_2 \times C_4$ (four elements of order 4, three elements of order 2)
- $C_2 \times C_2 \times C_2$ (with seven elements of order 2)

Every abelian group is a direct product of cyclic groups.

$$C_n = \text{cyclic group of order } n$$

(multiplicative)

$$C_n = \{1, g, g^2, \dots, g^{n-1}\}, \quad g^n = 1.$$



In a field of order q , the polynomial x^2-1 has at most 2 roots.
 (In $F[x]$, where F is any field, every polynomial of degree k has at most k roots.)
 If $f(x) \in F[x]$ has k roots $r_1, \dots, r_k \in F$, then $f(x) = \underbrace{(x-r_1)(x-r_2)\dots(x-r_k)}_{\text{degree } k} h(x)$

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

$$\mathbb{F}_5 = \mathbb{F}_5[\sqrt{2}] \neq \mathbb{F}_5[i], \quad i = \sqrt{-1} = \sqrt{4} = \pm 2$$

$1, \sqrt{2}$ is a basis

In \mathbb{F}_5 , -1 is already a square.

$$\mathbb{F}_5[i] = \mathbb{F}_5[2] = \mathbb{F}_5$$

$$\mathbb{Q}[\sqrt{4}] = \mathbb{Q}[2] = \mathbb{Q}$$

$$\mathbb{R}[\sqrt{2}] = \mathbb{R}$$

$$\mathbb{R}[i] = \mathbb{C}$$

In $\mathbb{R}[x]$, $\begin{cases} x^2-2 \text{ is reducible since } x^2-2 = (x+\sqrt{2})(x-\sqrt{2}). \\ x^2+1 \text{ is irreducible.} \end{cases}$

How do we extend \mathbb{F}_p to \mathbb{F}_{p^2} ? We want a quadratic extension $[\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$.
 A choice of basis is $\{1, \sqrt{a}\}$ if $a \in \mathbb{F}_p$ is not a square of any element in \mathbb{F}_p i.e. $x^2-a \in \mathbb{F}_p[x]$ should be irreducible.

When p is an odd prime, there are $p-1$ nonzero elements and half of them are squares, half are non-squares.

When $p=5$, the nonzero elements of \mathbb{F}_5 are $1, 2, 3, 4$ where $1, 4$ are squares; $2, 3$ are non-squares.

$$\mathbb{F}_{25} = \mathbb{F}_5[\sqrt{2}] = \mathbb{F}_5[\sqrt{3}].$$

When $p=2$, $x^2-a = (x-a)^2$ i.e. $x^2 = x \cdot x$ reducible

$$x^2-1 = (x-1)^2 \text{ reducible}$$

$\mathbb{F}_2 = \{0, 1\}$ has squares only.

But x^2+x+1 is irreducible in $\mathbb{F}_2[x]$

$$\mathbb{F}_4 = \mathbb{F}_2[x], \quad \alpha \text{ root of } x^2+x+1.$$

If $q = p^k$ then $\mathbb{F}_q \supset \mathbb{F}_p$ is an extension of degree $[\mathbb{F}_q : \mathbb{F}_p] = k$ with exactly k automorphisms.

In $\mathbb{F}_q = \mathbb{F}_3[i]$, the map $a+bi \mapsto a-bi$ is the nonidentity automorphism.

In $\mathbb{F}_{25} = \mathbb{F}_5[\sqrt{2}]$, the map $a+b\sqrt{2} \mapsto a-b\sqrt{2}$

$\mathbb{F}_4 = \mathbb{F}_2[x]$ the map $\begin{matrix} 0 \mapsto 0 \\ 1 \mapsto 1 \\ \alpha \mapsto \beta \\ \beta \mapsto \alpha \end{matrix}$
 $= \{0, 1, \alpha, \beta\}$
 $\alpha^2 = 1$

Finite fields are Galois extensions of their prime fields: $\mathbb{F}_q \supset \mathbb{F}_p$, $q = p^k$, p prime
 $[\mathbb{F}_q : \mathbb{F}_p] = k$ so $G = \text{Aut } \mathbb{F}_q$ has order $|G| = k$ and $G = \{1, \sigma, \sigma^2, \dots, \sigma^{k-1}\}$, $\sigma^k = 1$. Here $\sigma(x) = x^p$.

$\sigma(xy) = (xy)^p = x^p y^p = \sigma(x)\sigma(y)$ for all $x, y \in \mathbb{F}_q$.

$\sigma(x+y) = (x+y)^p = x^p + px^{p-1}y + \frac{p(p-1)}{2}x^{p-2}y^2 + \dots + px y^{p-1} + y^p$ by the Binomial Theorem $(x+y)^n = \sum_{i=0}^n \binom{n}{i} x^{n-i} y^i$
 where $\binom{n}{i} = \frac{n!}{i!(n-i)!}$, $n! = 1 \times 2 \times 3 \times \dots \times n$
 $\binom{n}{1} = \frac{n!}{1!(n-1)!} = n$
 $\binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}$
 $\binom{n}{0} = \frac{n!}{0!n!} = 1 = \binom{n}{n}$
divisible by p
 $= x^p + y^p = \sigma(x) + \sigma(y)$

$\sigma: \mathbb{F}_q \rightarrow \mathbb{F}_q$ is a homomorphism. **All elements of \mathbb{F}_q are roots of $x^q - x$.**

$\ker \sigma = \{x \in \mathbb{F}_q : \sigma(x) = 0\} = \{0\}$ so σ is one-to-one.

Since \mathbb{F}_q is finite, σ is onto. So σ is an isomorphism $\mathbb{F}_q \rightarrow \mathbb{F}_q$ i.e. σ is an automorphism of \mathbb{F}_q .

$\text{Aut } \mathbb{F}_q \supseteq \{1, \sigma, \sigma^2, \sigma^3, \dots\}$ but these automorphisms can't all be distinct

$$\sigma^k(x) = \underbrace{\sigma(\sigma(\sigma(\dots(\sigma(x))\dots))}_{k \text{ times}} = \underbrace{(((x^p)^p)^p)\dots)}_{k \text{ times}} = x^{p^k} = x^q = x$$

$\sigma^k = 1$

In $\mathbb{F}_q^* = \{x \in \mathbb{F}_q : x \neq 0\}$ is a multiplicative group (actually cyclic) of order $q-1$.
 $x^{q-1} = 1$ for all $x \in \mathbb{F}_q^*$

If $f(x) \in F[x]$ is irreducible, then we say any two roots α, β of $f(x)$ (typically in an extension field $E \supseteq F$) then α, β are conjugates.

Eg. $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ has roots $\pm\sqrt{2} \in \mathbb{R}$ or in $\mathbb{Q}[\sqrt{2}]$. $\pm\sqrt{2}$ are conjugates.

If $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ has roots $\pm i \in \mathbb{C}$ or $\mathbb{Q}[i]$. $\pm i$ are conjugates.

In E there can be an automorphism $\sigma \in \text{Aut } E$ fixing every element of F and mapping a root of $f(x)$ to any of its conjugates.

Eg. $f(x) = x^3 - 2$ has three roots $\alpha, \alpha\omega, \alpha\omega^2$ where $\alpha = \sqrt[3]{2}$, $\omega = e^{2\pi i/3} = \frac{-1 + \sqrt{3}i}{2}$, $\omega^2 = e^{4\pi i/3} = \frac{-1 - \sqrt{3}i}{2}$.

The elements $\alpha, \alpha\omega, \alpha\omega^2$ are conjugates. These are all the conjugates of α .

in $\mathbb{Q}[\alpha, \omega] \supset \mathbb{Q}$, $[\mathbb{Q}[\alpha, \omega] : \mathbb{Q}] = 6$.

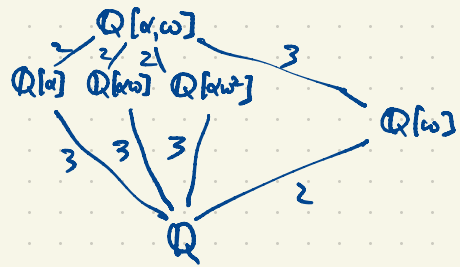
$$x^3 - 2 = (x - \alpha)(x - \alpha\omega)(x - \alpha\omega^2)$$

$\mathbb{Q}[\alpha, \omega]$ is the splitting field of $f(x) = x^3 - 2$

$\mathbb{Q}[\alpha]$ is not the splitting field of $f(x) = x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$

$$[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$$

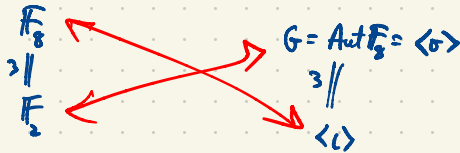
$$[\mathbb{Q}[\alpha\omega] : \mathbb{Q}] = 3$$



Eg. $\mathbb{F}_8 \supset \mathbb{F}_2 = \{0, 1\}$, $[\mathbb{F}_8 : \mathbb{F}_2] = 3 = |G|$ where $f = \text{Aut } \mathbb{F}_8 = \langle \sigma \rangle = \{1, \sigma, \sigma^2\}$, $\sigma^3 = 1$

$$\mathbb{F}_8 = \{a + b\gamma + c\gamma^2 : a, b, c \in \mathbb{F}_2\}, \quad \gamma^3 = \gamma + 1$$

$\{1, \gamma, \gamma^2\}$ basis



$$\begin{aligned} \sigma(x) &= x^2 \\ \sigma^2(x) &= (x^2)^2 = x^4 \\ \sigma^3(x) &= (x^4)^2 = x^8 = x \end{aligned}$$

x	$\sigma(x) = x^2$
0	0
1	1
γ	γ^2
γ^2	$\gamma^4 = \gamma + \gamma^2$
$\gamma^3 = \gamma + 1$	$\gamma^6 = 1 + \gamma^2$
γ^4	$\gamma^8 = \gamma$
$\gamma^5 = \gamma^2 + \gamma + 1$	$\gamma^{10} = \gamma^3 = \gamma + 1$
$\gamma^6 = 1 + \gamma^2$	$\gamma^{12} = \gamma^5 = \gamma^2 + \gamma + 1$
$\gamma^7 = 1$	1

$f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ is irreducible

It has roots in \mathbb{F}_8 : $\gamma, \gamma^2, \gamma^4$

$$\begin{aligned} f(x) &= x^3 + x + 1 = (x - \gamma)(x - \gamma^2)(x - \gamma^4) \\ &(\gamma^3 + \gamma + 1) = 0 \\ &\gamma^6 + \gamma^2 + 1 = 0 \end{aligned}$$

$\gamma^3 \in \mathbb{F}_8$ must have minimal poly. $g(x) \in \mathbb{F}_2[x]$ of degree 3. This must be $g(x) = x^3 + x^2 + 1$
 so $g(x) = x^3 + x^2 + 1$ must have roots $\gamma^3, \gamma^5, \gamma^6$

The roots of $x^8 - x \in \mathbb{F}_2[x]$ are all the eight elements of \mathbb{F}_8 .

$$\begin{aligned} x^8 - x &= x(x^7 - 1) = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) \\ &= x(x+1)(x^3 + x + 1)(x^3 + x^2 + 1) \\ &\quad 0 \quad 1 \quad \gamma, \gamma^2, \gamma^4 \quad \gamma^3, \gamma^5, \gamma^6 \end{aligned}$$

$$\begin{aligned} \sigma(\gamma^4) &= \gamma^8 = \gamma & \sigma(\gamma^5) &= \gamma^{10} = \gamma^3 \\ \sigma(\gamma^3) &= \gamma^6 & \sigma(\gamma^6) &= \gamma^{12} = \gamma^5 \end{aligned}$$

$$\mathbb{F}_5: \text{ all elements are roots of } x^5 - x = x(x^4 - 1) = x(x^2 - 1)(x^2 + 1) = x(x-2)(x-3)(x-1)(x+1)$$

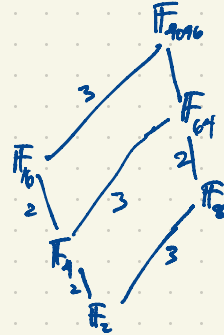
$$= x(x-1)(x-2)(x-3)(x-4)$$

0 1 2 3 4

Subfields of \mathbb{F}_{16} : $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8$

$$\begin{array}{c} \mathbb{F}_{16} \\ 2 | \\ \mathbb{F}_4 \\ 2 | \\ \mathbb{F}_2 \end{array}$$

$$[\mathbb{F}_8 : \mathbb{F}_2] = 3$$



Math 4550 Spring 2025 = 45² Theory of Numbers
 Putnam Exam 2024 Dec 7 8:30 am - 4:30 pm
 Interested? Email me with 'Putnam' in subject line.

More examples of fields: $F((x)) \supset F(x) \supset F$ where F is a field.

Laurant series in x
with coefficients in F

rational functions in x
with coefficients in F

x is an indeterminate
(a symbol)

Eg. $f(x) = \frac{x}{1-x-x^2} \in \mathbb{Q}(x)$ can be regarded as an infinite series in x with coefficients in \mathbb{Q}

$$= F_0 + F_1 x + F_2 x^2 + F_3 x^3 + \dots \quad \text{where } F_i \in \mathbb{Q}$$

$$f'(x) = \frac{(1-x-x^2) - x(-1-2x)}{(1-x-x^2)^2} = \frac{1+x^2}{(1-x-x^2)^2}$$

$$f''(x) = \frac{(1-x-x^2)^2(2x) - (1+x^2)2(1-x-x^2)(-1-2x)}{(1-x-x^2)^4} = \frac{(1-x-x^2)(2x) + 2(1+x^2)(1+2x)}{(1-x-x^2)^3} = \frac{2x-2x^2-2x^3 + 2(1+2x+x^2+2x^3)}{(1-x-x^2)^3}$$

$$= \frac{2+6x+2x^3}{(1-x-x^2)^3}$$

$$f'''(x) = \text{etc.}$$

$$f^{(n)}(x) = f^{(n)}(x) = \text{etc.}$$

Taylor series centered at 0 for $f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n = f(0) + f'(0)x + \frac{f''(0)}{2}x^2 + \frac{f'''(0)}{6}x^3 + \frac{f^{(4)}(0)}{24}x^4 + \dots$

$$= 0 + 1x + \frac{2}{2}x^2 + \frac{12}{6}x^3 + \frac{72}{24}x^4 + \dots$$

$$= x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + 13x^7 + \dots$$

The Fibonacci sequence F_n is defined recursively

$$F_n = \begin{cases} 0, & \text{if } n=0 \\ 1, & \text{if } n=1 \\ F_{n-1} + F_{n-2}, & \text{if } n \geq 2 \end{cases}$$

Alternatively: $f(x) = \frac{x}{1-x-x^2} = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + \dots = x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + \dots$

$$x = (1-x-x^2)(a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + \dots)$$

$$= \underbrace{a_0}_0 + \underbrace{(a_1 - a_0)}_1 x + \underbrace{(a_2 - a_1 - a_0)}_0 x^2 + \underbrace{(a_3 - a_2 - a_1)}_0 x^3 + \underbrace{(a_4 - a_3 - a_2)}_0 x^4 + \dots$$

Third way: $\frac{1}{1-u} = 1 + u + u^2 + u^3 + u^4 + \dots$ (geometric series)

Since $(1-u)(1+u+u^2+u^3+u^4+\dots) = 1 - \cancel{u} + \cancel{u} - \cancel{u^2} + \cancel{u^2} - \cancel{u^3} + \cancel{u^3} + \dots = 1$

Substitute $u = x+x^2$

$$\frac{x}{1-x-x^2} = x(1 + (x+x^2) + (x+x^2)^2 + (x+x^2)^3 + (x+x^2)^4 + \dots)$$

$$= x(1 + (x+x^2) + (x^2+2x^3+x^4) + (x^3+3x^4+3x^5+x^6) + (x^4+4x^5+6x^6+4x^7+x^8) + \dots)$$

$$= x(1 + x + 2x^2 + 3x^3 + 5x^4 + \dots)$$

$$= x + x^2 + 2x^3 + 3x^4 + 5x^5 + \dots$$

Fourth method:

$$\frac{x}{1-x-x^2} = \frac{x}{(1-\alpha x)(1-\beta x)} = \frac{A}{1-\alpha x} + \frac{B}{1-\beta x} \Rightarrow x = A(1-\beta x) + B(1-\alpha x)$$

(for $x = \frac{1}{\alpha}$) $\frac{1}{\alpha} = A(1 - \frac{\beta}{\alpha}) \Rightarrow 1 = A(\frac{\alpha - \beta}{\alpha}) \Rightarrow A = \frac{\alpha}{\alpha - \beta} = \frac{1}{\alpha - \beta}$

(for $x = \frac{1}{\beta}$) $\frac{1}{\beta} = B(1 - \frac{\alpha}{\beta}) \Rightarrow 1 = B(\frac{\beta - \alpha}{\beta}) \Rightarrow 1 = \frac{B(\beta - \alpha)}{\beta} = \frac{B(-1)}{\beta} \Rightarrow B = -\frac{1}{\beta}$

α, β are the reciprocal roots of $1-x-x^2 = x^2(x^{-1}-x-1)$

$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}, \quad \alpha - \beta = \sqrt{5}$$

$\approx 1.618, \quad \approx -0.618$

$$\frac{x}{1-x-x^2} = \frac{x}{(1-\alpha x)(1-\beta x)} = \frac{1}{\sqrt{5}} \left(\frac{1}{1-\alpha x} - \frac{1}{1-\beta x} \right) = \frac{1}{\sqrt{5}} \left(\sum_{n=0}^{\infty} \alpha^n x^n - \sum_{n=0}^{\infty} \beta^n x^n \right) = \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} (\alpha^n - \beta^n) x^n = \sum_{n=0}^{\infty} F_n x^n = x + x^2 + 2x^3 + 3x^4 + 5x^5 + \dots$$

where $F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$

$\frac{1}{\sqrt{5}} \rightarrow \alpha$ $F_n \sim \frac{1}{\sqrt{5}} \alpha^n$ $F_n = \frac{\alpha^n}{\sqrt{5}}$ rounded to the nearest integer.

$|\beta| < 1$ so $\beta^n \rightarrow 0$
 $|\alpha| > 1$ so $\alpha^n \rightarrow$ no grows exponentially

Ex. Count the number a_n of sequences of 0's and 1's of length n having no two consecutive 1's.

n		
0	''	$a_0 = 1$
1	'0', '1'	$a_1 = 2$
2	00, 10, 01	$a_2 = 3$
3	000, 100, 010, 001, 101	$a_3 = 5$
4	-----	$a_4 = 8$

Other series are relevant in combinatorial applications in which $f(x)$ cannot converge anywhere eg.

$$f(x) = \sum_{n=0}^{\infty} n! x^n = 1 + x + 2x^2 + 6x^3 + 24x^4 + \dots$$



$$f(x)^2 = (1 + x + 2x^2 + 6x^3 + \dots)^2 = 1 + 2x + 5x^2 + \dots$$

$$\frac{f(x)}{x} = \frac{1}{x} + 1 + 2x + 6x^2 + 24x^3 + \dots$$



$$\frac{x}{1-x-x^2} = x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + \dots$$

$$\frac{1}{1-x-x^2} = 1 + x + 2x^2 + 3x^3 + \dots$$

$$\frac{1}{x-x^2-x^3} = \frac{1}{x} + 1 + 2x + 3x^2 + 5x^3 + \dots$$

What is a series $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots$ really?

We think of f as the sequence $(a_0, a_1, a_2, a_3, \dots)$

So if $g(x) = b_0 + b_1x + b_2x^2 + \dots$ then g is really g is $(b_0, b_1, b_2, b_3, \dots)$

$f+g = (a_0+b_0, a_1+b_1, a_2+b_2, a_3+b_3, \dots)$ entrywise addition

$fg = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0, \dots)$
multiplication is by convolution (not entrywise)

$$fg = (c_0, c_1, c_2, c_3, \dots), \quad c_n = \sum_{k=0}^n a_k b_{n-k}$$

$F[[x]] =$ power series in x with coefficients in F (a ring)

$F((x)) =$ field of quotients of $F[[x]]$ (like $F[[x]]$ but with some negative powers of x)

eg. $F = \mathbb{F}_2 = \{0, 1\}$

$$\frac{x^2 + x^4 + x^5 + x^7 + \dots}{x^5 + x^6 + x^9 + x^{11} + \dots} = x^{-3} + x^{-2} + 1 + \dots \quad (\text{higher degree terms})$$

$$x^2 + x^4 + x^5 + x^7 + \dots = (x^5 + x^6 + x^9 + x^{11} + \dots) (x^{-3} + x^{-2} + 1 + \underbrace{\underbrace{\underbrace{\underbrace{0x^2 \dots}_{0x}}_{x^0=1}}_{0x^{-1}}}_{1x^{-2}} \dots)$$

In the ring $F[[x]]$, the units (ie. invertible elements) are all the elements with nonzero constant term.

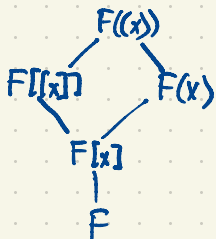
$F((x))$ is however a field ie. all nonzero elements are units

Why can't we allow infinitely many powers of x with negative exponents as well as positive exponents?

$(\dots + x^{-3} + x^{-2} + x^{-1} + 1 + x + x^2 + x^3 + \dots) (\dots + 5x^{-3} + 2x^{-2} + 7x^{-1} + 11 + 13x + 2x^2 + 3x^3 + x^4 + \dots)$ is undefined whereas

$$(x^{-2} + x^{-1} + 1 + x + x^2 + x^3 + \dots) (7x^{-1} + 11 + 13x + 2x^2 + 3x^3 + x^4 + \dots) = 7x^{-3} + 18x^{-2} + 31x^{-1} + 33 + 36x + \dots$$

$$\frac{1}{x^2 + x^3} \stackrel{F(x)}{=} \frac{1}{x^2(1+x)} = \frac{1}{x^2} (1 - x + x^2 - x^3 + x^4 - x^5 + \dots) = x^{-2} - x^{-1} + 1 - x + x^2 - x^3 + x^4 - x^5 + \dots$$



Automorphisms of $\mathbb{Q}(x) \supset \mathbb{Q}$ includes $f(x) \mapsto f(x+i)$

has inverse $f(x) \mapsto f(x-i)$

$$f(x)+g(x) \mapsto f(x+i) + g(x+i)$$

$$f(x)g(x) \mapsto f(x+i)g(x+i)$$

$$[\mathbb{Q}(x) : \mathbb{Q}] = \infty \quad (\text{actually } \aleph_0)$$

This is a start on one of the HW4 problems.

How about square roots?

For $f(x) \in \mathbb{Q}(x)$, when does $\sqrt{f(x)} \in \mathbb{Q}(x)$?

$\sqrt{x} \notin \mathbb{Q}(x)$. Very small fraction of functions $f(x) \in \mathbb{Q}(x)$ have $\sqrt{f(x)} \in \mathbb{Q}(x)$.

eg. if $F = \mathbb{Q}(x)$ then $E = F(\sqrt{x}) = \mathbb{Q}(x, \sqrt{x}) = \mathbb{Q}(\sqrt{x})$ since $x \in \mathbb{Q}(\sqrt{x})$, in fact $x \in \mathbb{Q}[\sqrt{x}]$.

$$\sqrt{1+x} \in \mathbb{Q}(\!(x)\!)$$

$$\sqrt{1+x} = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots, \quad a_i \in \mathbb{Q}$$
$$\in \mathbb{Q}[\![x]\!]$$

$$1+x = (a_0 + a_1x + a_2x^2 + a_3x^3 + \dots)^2 = a_0^2 + 2a_0a_1x + (a_1^2 + 2a_0a_2)x^2 + (2a_0a_3 + 2a_1a_2)x^3 + (a_2^2 + 2a_1a_3 + 2a_0a_4)x^4 + \dots$$

$$a_0 = \pm 1. \quad \text{Let's take } a_0 = 1. \quad = 1 + 2a_1x + (a_1^2 + 2a_2)x^2 + (2a_3 + 2a_1a_2)x^3 + (a_2^2 + 2a_1a_3 + 2a_4)x^4 + \dots$$

$$\text{Now } a_1 = \frac{1}{2} \quad = 1 + x + \underbrace{(\frac{1}{4} + 2a_2)}_0 x^2 + \underbrace{(2a_3 + a_2)}_0 x^3 + (a_2^2 + a_3 + 2a_4)x^4 + \dots$$

$$a_2 = -\frac{1}{8}$$

$$a_3 = \frac{1}{16}$$

etc.

$$\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \dots$$

The two square roots of $1+x$ in $\mathbb{Q}[\![x]\!]$ are $\pm\sqrt{1+x} = \pm(1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \dots)$

Binomial Theorem

$$(1+x)^a = \sum_{k=0}^{\infty} \binom{a}{k} x^k$$

$$\binom{a}{k} = \frac{a(a-1)(a-2)\dots(a-k+1)}{k(k-1)(k-2)\dots 2 \cdot 1} \leftarrow k!$$

$k \in \{0, 1, 2, \dots\}$
 $a \in \mathbb{R}$.

(Polynomial of degree k in a ;
but if $a \in \{0, 1, 2, \dots\}$ then this value $\binom{a}{k}$ is entry k in row a of Pascal's triangle).

$$\sqrt{1+x} =$$

$$(1+x)^{\frac{1}{2}} = 1 + \frac{\frac{1}{2}}{\binom{\frac{1}{2}}{1}} x + \frac{\frac{1}{2}(\frac{1}{2}-1)}{\binom{\frac{1}{2}}{2}} x^2 + \frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2)}{\binom{\frac{1}{2}}{3}} x^3 + \frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2)(\frac{1}{2}-3)}{\binom{\frac{1}{2}}{4}} x^4 + \dots$$

$$= 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \frac{5}{128}x^4 + \dots \in \mathbb{Q}[[x]]$$

$$-\frac{5}{8} \cdot \frac{1}{16} = -\frac{5}{128}$$

$$\sqrt{2+x} = \sqrt{2} \sqrt{1+\frac{x}{2}} \in \mathbb{R}[[x]] \notin \mathbb{Q}[[x]]$$

On HW4 about #3 (?)

$$\sqrt{4+x} = 2\sqrt{1+\frac{x}{4}} \in \mathbb{Q}[[x]]$$

If $q = p^k$, p prime $k \geq 1$ we have a field of order q , unique up to isomorphism, denoted \mathbb{F}_q .

First suppose q is odd i.e. $p = \text{char } \mathbb{F}$ is odd.
Half the nonzero elements are squares.

"ABLE WAS I ERE I SAW ECB"

Eg. $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$$\mathbb{F}_{49} = \mathbb{F}_7[\sqrt{3}] = \mathbb{F}_7[\sqrt{5}] = \mathbb{F}_7[\sqrt{6}] = \mathbb{F}_7[i], i^2 = -1$$

$x^2 - a$ is reducible iff a is a square.

$x^2 - a$ is irreducible iff $\mathbb{F}[\sqrt{a}] > \mathbb{F}$ is a quadratic extension.

If $q = 2^k$ then every element of \mathbb{F}_q has a unique square root and $x \mapsto \sqrt{x}$ is an automorphism of \mathbb{F}_q .

a	a^2	a	a^2
0	0	0	0
1	1	±1	1
2	4	±2	4
3	9	±3	9
4	16		
5	25		
6	36		