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. $G = \mathrm{Aut}\, E$ satisfies $|G| = n$; but in general $|G| \le n$.)

Back to basics:

In a field F, if $\underbrace{1+1+1+\cdots+1}_{n\geq 1} = 0$ 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

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

By minimality of n, n is prime.

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

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

- If $\mathrm{char}\, F = p$ then $F \supseteq \mathbb{F}_p$ = field of order p ($\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \cdots, p-1\}$ = "integers mod p").
  eg. $\mathbb{F}_p$, $\mathbb{F}_{p^2}, \mathbb{F}_{p^3}, \mathbb{F}_{p^4}, \cdots$, $\mathbb{F}_p(x) = \{$all rational functions in x with coefficients in $\mathbb{F}_p\}$, $\cdots$

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

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 <u>degree</u> $[E:F]$ of this extension eg.

$[\mathbb{C}:\mathbb{R}] = 2$ $\quad$ $\{1, i\}$ basis

$[\mathbb{R}:\mathbb{Q}] = \infty$ $\quad$ $1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{10}, \sqrt{11}, \dots$ 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 <u>unique</u> 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

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

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

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

$\mathbb{F}_4 \supset \mathbb{F}_2$ of degree $[\mathbb{F}_4 : \mathbb{F}_2] = 2$ with basis $1, \alpha$

$$\mathbb{F}_4 = \{a \cdot 1 + b\alpha \;:\; a, b \in \mathbb{F}_2\} = \{0, 1, \alpha, 1+\alpha\} = \{0, 1, \alpha, \underset{\beta}{\underset{\parallel}{\alpha^2}}\}$$ where $\alpha^2 = \alpha + 1$.

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

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: $\underbrace{\underset{x\cdot x}{\overset{\shortparallel}{x^2}},\ \underset{(x+1)(x+1)}{\overset{\shortparallel}{x^2+1}},\ \underset{x(x+1)}{\overset{\shortparallel}{x^2+x}}}_{\text{reducible}}$, x^2+x+1 irreducible

degree 3:
$$\begin{aligned}
x^3 &= x\cdot x\cdot x\\
x^3+1 &= (x+1)(x^2+x+1)\\
x^3+x &= x\cdot(x+1)^2\\
x^3+x+1 &\quad \text{irreducible}\\
x^3+x^2 &= x\cdot x\cdot(x+1)\\
x^3+x^2+1 &\quad \text{irreducible}\\
x^3+x^2+x &= x(x^2+x+1)\\
x^3+x^2+x+1 &= (x+1)^3
\end{aligned}$$

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

Let α be a root of x^2+x+1. The other root is $\alpha+1$.
$$\alpha^2+\alpha+1=0 \implies \alpha^2 = -\alpha-1 = \alpha+1$$

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 i.e. $\gamma^3 = \gamma+1$
$$\begin{aligned}
&= \{a\cdot 1 + b\cdot\gamma + c\cdot\gamma^2 : a,b,c\in\mathbb{F}_2\}.\\
&= \{0, 1, \gamma, \underset{\gamma^3}{\overset{\shortparallel}{\gamma+1}}, \gamma^2, \underset{\gamma^6}{\overset{\shortparallel}{\gamma^2+1}}, \underset{\gamma^4}{\overset{\shortparallel}{\gamma^2+\gamma}}, \underset{\gamma^5}{\overset{\shortparallel}{\gamma^2+\gamma+1}}\}.
\end{aligned}$$

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

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 $\mathbb{F}_8$: $\gamma^3, \gamma^5, \gamma^6 = \gamma^{-1}$

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 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 $\alpha_1, \ldots, \alpha_k$ be a basis for $\mathbb{F}_q$ over $\mathbb{F}_p$ i.e. $\mathbb{F}_q = \{a_1\alpha_1 + a_2\alpha_2 + \cdots + a_k\alpha_k : a_1,\ldots,a_k \in \mathbb{F}_p\}$.
$$q = |\mathbb{F}_q| = p^k$$

$\mathbb{F}_9 = \mathbb{F}_3[i]$ compare: $\mathbb{C} = \mathbb{R}[i]$, $\mathbb{Q}[i] \supset \mathbb{Q}$, $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$, $i = \sqrt{-1}$. $\{1, i\}$ is a basis of the extension in each case.

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

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

$\phantom{= \{}0,\ 1 = \theta^8,\ 2 = \theta^4,\ i = \theta^6,\ 1+i = \theta,\ 2+i = \theta^7,\ 2i = \theta^2,\ 1+2i = \theta^3,\ 2+2i = \theta^5$

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

$\theta^0 = 1$

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

$\theta^2 = (1+i)^2 = \cancel{1} + 2i + \cancel{i^2} = 2i$

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

$\theta^4 = \theta^3 \cdot \theta = (1+2i)(1+i) = 1-2 = -1 = 2$

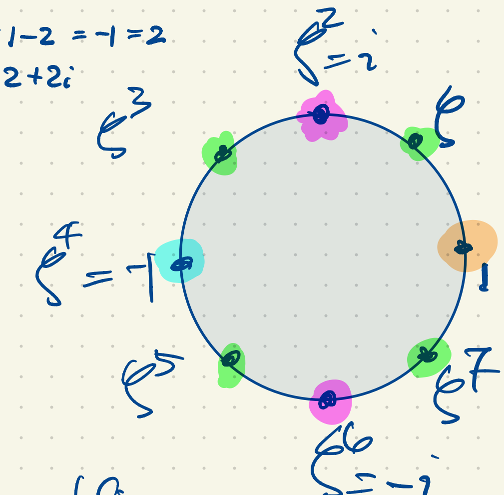
$\theta^5 = \theta^4 \cdot \theta = -\theta = 2\theta = 2+2i$

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

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

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

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



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, two elements of order 4, 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 = cyclic group of order n (multiplicative)

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

In a field of order 9, 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 $\underbrace{f(x)}_{\text{degree } k} = (x-r_1)(x-r_2)\cdots(x-r_k)h(x)$

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

$\mathbb{F}_{25} = \mathbb{F}_5[\sqrt{2}] \neq \mathbb{F}_5[i]$, $i = \sqrt{-1} = \sqrt{4} = \pm 2$

$1, \sqrt{2}$ 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 nonsquares.
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. $\underbrace{x^2 = x \cdot x}_{\text{reducible}}$, $\underbrace{x^2-1 = (x-1)^2}_{\text{reducible}}$

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

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

$\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, α 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 $\mathbb{F}_9 = \mathbb{F}_3[i]$, the map $a+bi \mapsto a-bi$ is the non-identity automorphism.

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

$\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ the map $0 \mapsto 0$, $1 \mapsto 1$, $\alpha \mapsto \beta$, $\beta \mapsto \alpha$. - - - - - . .

$= \{0, 1, \alpha, \beta\}$, $\beta = \alpha+1 = \alpha^2$

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

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

$\sigma(x+y) = (x+y)^p = x^p + \underbrace{px^{p-1}y + \frac{p(p-1)}{2}x^{p-2}y^2 + \cdots + pxy^{p-1}}_{\text{divisible by } p} + y^p$ by the Binomial Theorem $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$

where $\binom{n}{i} = \frac{n!}{i!(n-i)!}$, $n! = 1\times 2\times 3\times \cdots \times n$

$\binom{n}{1} = \frac{n!}{1!(n-1)!} = n$

$\binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}$

$\binom{n}{0} = \frac{n!}{0!\,n!} = 1 = \binom{n}{n}$

$= x^p + y^p = \sigma(x) + \sigma(y)$

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

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

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

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

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

$\sigma^k = \iota$

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

Eg. $\mathbb{F}_4 > \mathbb{F}_2$ of degree $[\mathbb{F}_4 : \mathbb{F}_2] = 2$ with basis $\{1, \alpha\}$

$\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$ where $\beta = \alpha^2 = \alpha + 1$

$= \{a\cdot 1 + b\cdot \alpha : a, b \in \mathbb{F}_2\}$

$\mathrm{Aut}\,\mathbb{F}_4 = \langle \sigma \rangle = \{\iota, \sigma\}$.

x	$\sigma(x) = x^2$	$\sigma^2(x) = x^4$
0	0	0
1	1	1
α	β	α
β	α	β

$$\begin{tikzcd} \mathbb{F}_4 \arrow[d, dash, "2"'] & G = \langle\sigma\rangle = \{\iota, \sigma\} \arrow[d, dash, "2"] \\ \mathbb{F}_2 & \langle \iota \rangle \end{tikzcd}$$

Eg. $\mathbb{F}_9 \supset \mathbb{F}_3 = \{0, 1, 2\}$, $[\mathbb{F}_9 : \mathbb{F}_3] = 2$ with basis $\{1, i\}$

$\mathbb{F}_9 = \{a + bi : a, b \in \mathbb{F}_3\}$

$i = \sqrt{-1} = \sqrt{2}$

$\sigma(x) = x^3$

$\sigma(a+bi) = a - bi$ for $a, b \in \mathbb{F}_3$

x	$\sigma(x) = x^3$
0	0
1	1
2	2
i	$-i = 2i$
$2i$	$-2i = i$
$a+bi$	$a-bi$

$(a+bi)^3 = a^3 + \cancel{3a^2bi} + \cancel{3a(bi)^2} + (bi)^3$

$= a - bi$

$$\begin{tikzcd} \mathbb{F}_9 \arrow[d, dash, "2"'] & G = \langle\sigma\rangle = \{\iota, \sigma\} \arrow[d, dash, "2"] \\ \mathbb{F}_3 & \langle \iota \rangle \end{tikzcd}$$

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

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

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

$\sigma(x) = x^2$,

$\sigma^2(x) = (x^2)^2 = x^4$

$\sigma^3(x) = ((x^2)^2)^2 = x^8 = x$

x	$\sigma(x) = x^2$
0	0
1	1
γ	γ^2
γ^2	$\gamma^4 = \gamma + \gamma^2$
$\gamma^3 = 1 + \gamma$	$\gamma^6 = 1 + \gamma^2$
$\gamma^4 = \gamma + \gamma^2$	γ
$\gamma^5 = \gamma^2 + \gamma + 1$	$\gamma^3 = 1 + \gamma$
$\gamma^6 = 1 + \gamma^2$	$\gamma^5 = \gamma^2 + \gamma + 1$
$\gamma^7 = 1$	1

$$\begin{tikzcd} \mathbb{F}_8 \arrow[d, dash, "3"'] & G = \mathrm{Aut}\,\mathbb{F}_8 = \langle\sigma\rangle \arrow[d, dash, "3"] \\ \mathbb{F}_2 & \langle \iota \rangle \end{tikzcd}$$

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 $\sigma \in \operatorname{Aut} E$ 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 $\alpha = \sqrt[3]{2}$, $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$, $\omega^2 = e^{4\pi i/3} = \frac{-1-\sqrt{-3}}{2}$.

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

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

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

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

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

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

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

$$\begin{tikzcd}
 & & \mathbb{Q}[\alpha,\omega] \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"] \arrow[d, dash, "2"] \arrow[dr, dash, "3"] & \\
\mathbb{Q}[\alpha] \arrow[drr, dash, "3"'] & \mathbb{Q}[\alpha\omega] \arrow[dr, dash, "3"] & \mathbb{Q}[\alpha\omega^2] \arrow[d, dash, "3"] & \mathbb{Q}[\omega] \arrow[dl, dash, "2"] \\
 & & \mathbb{Q} &
\end{tikzcd}$$

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

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

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

$$\begin{array}{ccc} \mathbb{F}_8 & & G = \mathrm{Aut}\,\mathbb{F}_8 = \langle\sigma\rangle \\ 3\,\| & & 3\,\| \\ \mathbb{F}_2 & & \langle\iota\rangle \end{array}$$

$\sigma(x) = x^2$,

$\sigma^2(x) = (x^2)^2 = x^4$

$\sigma^3(x) = ((x^2)^2)^2 = x^8 = x$

x	$\sigma(x) = x^2$
0	0
1	1
γ	γ^2
γ^2	$\gamma^4 = \gamma + \gamma^2$
$\gamma^3 = 1 + \gamma$	$\gamma^6 = 1 + \gamma^2$
$\gamma^4 = \gamma + \gamma^2$	γ
$\gamma^5 = \gamma^2 + \gamma + 1$	$\gamma^3 = 1 + \gamma$
$\gamma^6 = 1 + \gamma^2$	$\gamma^5 = \gamma^2 + \gamma + 1$
$\gamma^7 = 1$	1

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

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

$\sigma(\gamma^4) = \gamma^8 = \gamma$

$\sigma(\gamma^5) = \gamma^{10} = \gamma^3$

$\sigma(\gamma^3) = \gamma^6$

$\sigma(\gamma^6) = \gamma^{12} = \gamma^5$

$f(x) = x^3 + x + 1 = (x - \gamma)(x - \gamma^2)(x - \gamma^4)$

$(\gamma^3 + \gamma + 1)^2 = 0$

$\gamma^6 + \gamma^2 + 1 = 0$

$\gamma^3 \in \mathbb{F}_8$ 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 $\gamma^3, \gamma^6, \gamma^5$

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

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

$0 \quad 1 \quad \gamma, \gamma^2, \gamma^4 \quad \gamma^3, \gamma^5, \gamma^6$

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

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

$0 \quad 1 \quad 2 \quad 3 \quad 4$

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

$$\begin{tikzcd}
\mathbb{F}_{16} \arrow[d, dash, "2"'] \\
\mathbb{F}_4 \arrow[d, dash, "2"'] \\
\mathbb{F}_2
\end{tikzcd}$$

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

$$\begin{tikzcd}
& & \mathbb{F}_{4096} \arrow[dll, dash, "3"'] \arrow[dr, dash] & & \\
\mathbb{F}_{16} \arrow[dr, dash, "2"'] & & & \mathbb{F}_{64} \arrow[dll, dash, "3"] \arrow[dr, dash, "2"] & \\
& \mathbb{F}_4 \arrow[dr, dash, "2"'] & & & \mathbb{F}_8 \arrow[dll, dash, "3"] \\
& & \mathbb{F}_2 & &
\end{tikzcd}$$

Math 4550 Spring $2025 = 45^2$ 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.

Laurent series in x with coefficients in F ; rational functions in x with coefficients in F ; x is an indeterminate (a symbol)

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

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

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

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

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

$f'''(x) =$ etc.

$f^{(4)}(x) = f^{IV}(x) =$ etc.

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

$= 0 + 1x + \underbrace{\frac{2}{2}}_{}\overset{1}{} x^2 + \frac{12}{6}x^3 + \frac{72}{24}x^4 + \cdots$

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

The Fibonacci sequence F_n is defined recursively by

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

Alternatively: $f(x) = \frac{x}{1-x-x^2} = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + \cdots = x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + \cdots$

$a_0 = 0$, $a_1 = 1$, $a_2 = 1$

$$x = (1-x-x^2)(a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + \cdots)$$

$$= \underbrace{a_0}_{=0} + (\underbrace{a_1 - \cancel{a_0}}_{=1})x + (\underbrace{a_2 - a_1 - \cancel{a_0}}_{=0})x^2 + (\underbrace{a_3 - a_2 - a_1}_{=0})x^3 + (\underbrace{a_4 - a_3 - a_2}_{=0})x^4 + \cdots$$

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

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

Substitute $u = x + x^2$

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

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

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

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

Fourth method:

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

(for $x = \frac{1}{\alpha}$) $\frac{1}{\alpha} = A\left(1 - \frac{\beta}{\alpha}\right) \Rightarrow 1 = A(\alpha-\beta) \Rightarrow A = \frac{1}{\alpha-\beta} = \frac{1}{\sqrt{5}}$

(for $x = \frac{1}{\beta}$) $\frac{1}{\beta} = B\left(1 - \frac{\alpha}{\beta}\right) \Rightarrow 1 = B(\beta-\alpha) = B(-\sqrt{5}) \Rightarrow B = -\frac{1}{\sqrt{5}}$

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

$\alpha = \frac{1+\sqrt{5}}{2} \approx 1.618$, $\beta = \frac{1-\sqrt{5}}{2} \approx -0.618$, $\alpha - \beta = \sqrt{5}$

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

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

$|\beta| < 1$ so $\beta^n \to 0$ decays exponentially

$|\alpha| > 1$ so $\alpha^n \to \infty$ grows ...

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

Eg. 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.

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

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

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

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

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

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