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 ($\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$ = "integers mod p").

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

- 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 __degree__ $[E:F]$ of this extension eg.

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

$[\mathbb{R}:\mathbb{Q}] = \infty$
$1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{10}, \sqrt{11}, \ldots$ 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: $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_8, \mathbb{F}_9, \mathbb{F}_{11}, \mathbb{F}_{13}, \mathbb{F}_{16}, \mathbb{F}_{17}, \ldots$

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

$+$	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 $1, \alpha$

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

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

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

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

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

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

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

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

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

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

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.

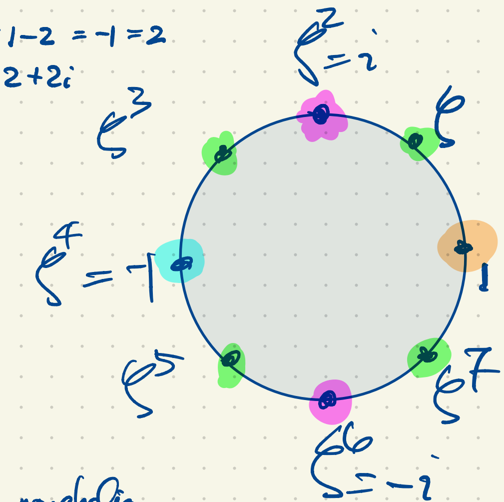
$= \{a+bi : a,b \in \mathbb{F}_3\}$

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

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

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

$$\theta^0 = 1$$
$$\theta^1 = \theta = 1+i$$
$$\theta^2 = (1+i)^2 = \cancel{1} + 2i + \cancel{i^2} = 2i$$
$$\theta^3 = \underbrace{2i}_{\theta^2}\underbrace{(1+i)}_{\theta} = -2+2i = 1+2i$$
$$\theta^4 = \theta^3 \cdot \theta = (1+2i)(1+i) = 1-2 = -1 = 2$$
$$\theta^5 = \theta^4 \cdot \theta = -\theta = 2\theta = 2+2i$$
$$\theta^6 = \theta^4 \cdot \theta^2 = -\theta^2$$
$$\theta^7 = \theta^4 \cdot \theta^3 = -\theta^3$$
$$\theta^8 = \theta^4 \cdot \theta^4 = -\theta^4$$



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

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 ... $a+b\sqrt{2} \mapsto a-b\sqrt{2}$ . . . .

$$\mathbb{F}_4 = \mathbb{F}_2[\alpha] = \{0,1,\alpha,\beta\} \qquad \text{the map} \quad \begin{array}{l} 0 \mapsto 0 \\ 1 \mapsto 1 \\ \alpha \mapsto \beta \\ \beta \mapsto \alpha \end{array} \quad \ldots\ldots$$

$$\beta = \alpha+1 = \alpha^2$$

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

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

$$\sigma(x+y) = (x+y)^p = x^p + \underbrace{px^{p-1}y + \cancel{\tfrac{p(p-1)}{2}}x^{p-2}y^2 + \cdots + pxy^{p-1}}_{\text{divisible by } p} + y^p$$
$$= x^p + y^p = \sigma(x)+\sigma(y)$$

by the Binomial Theorem $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i}y^i$

where $\binom{n}{i} = \frac{n!}{i!(n-i)!}$, $n! = 1\times2\times3\times\cdots\times n$

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

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

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

$\sigma:\mathbb{F}_q\to\mathbb{F}_q$ 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 $\mathbb{F}_q$.

$\operatorname{Aut}\mathbb{F}_q \supseteq \{\iota,\sigma,\sigma^2,\sigma^3,\ldots\}$ 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. $\mathbb{F}_4 \supset \mathbb{F}_2$ of degree $[\mathbb{F}_4 : \mathbb{F}_2] = 2$ with basis $\{1, \alpha\}$

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

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

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

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

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

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

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

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

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

$\sigma(x) = x^3$

$\sigma(a+bi) = a - bi$

for $a, b \in \mathbb{F}_3$

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

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

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

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

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

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

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

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

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

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

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

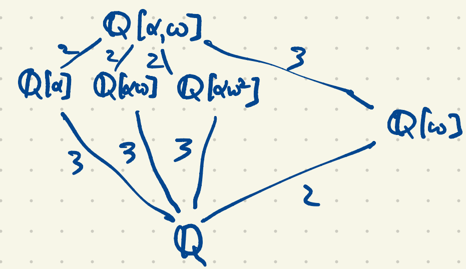
$x^3 - 2 = (x-\alpha)(x-\alpha\omega)(x-\alpha\omega^2)$

$\mathbb{Q}[\alpha,\omega]$ 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 $G = \mathrm{Aut}\,\mathbb{F}_8 = \langle \sigma \rangle = \{\iota, \sigma, \sigma^2\}$, $\sigma^3 = \iota$

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

$\{1, \gamma, \gamma^2\}$ 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 $\mathbb{F}_8$: $\gamma, \gamma^2, \gamma^4$

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

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

$$(\gamma^3 + \gamma + 1)^2 = 0$$
$$\gamma^6 + \gamma^2 + 1 = 0$$

$\sigma(\gamma^3) = \gamma^6$ $\qquad \sigma(\gamma^5) = \gamma^{10} = \gamma^3$

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

$\gamma^3 \in \mathbb{F}_8$ 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 $\mathbb{F}_8$.

$$x^8 - x = x(x^7 - 1) = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$
$$= \underbrace{x}_{0}\,\underbrace{(x+1)}_{1}\,\underbrace{(x^3 + x + 1)}_{\gamma,\,\gamma^2,\,\gamma^4}\,\underbrace{(x^3 + x^2 + 1)}_{\gamma^3,\,\gamma^5,\,\gamma^6}$$

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

$$= \underset{0}{x}\,\underset{1}{(x-1)}\,\underset{2}{(x-2)}\,\underset{3}{(x-3)}\,\underset{4}{(x-4)}$$

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

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

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

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

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 $\mathbb{Q}$

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

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

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

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

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

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

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

$$= 0 + 1x + \underset{\text{"1}}{\frac{2}{2}}x^2 + \frac{12}{6}x^3 + \frac{72}{24}x^4 + \cdots$$

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

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

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

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

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

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 $x = \frac{1}{\alpha}$) $\frac{1}{\alpha} = A\left(1 - \frac{\beta}{\alpha}\right) \Rightarrow 1 = A(\alpha - \beta) \Rightarrow A = \frac{1}{\alpha-\beta} = \frac{1}{\sqrt5}$

(for $x = \frac{1}{\beta}$) $\frac{1}{\beta} = B\left(1 - \frac{\alpha}{\beta}\right) \Rightarrow 1 = B(\beta - \alpha) = B(-\sqrt5) \Rightarrow B = -\frac{1}{\sqrt5}$

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

$\alpha = \frac{1+\sqrt5}{2} \approx 1.618$, $\beta = \frac{1-\sqrt5}{2} \approx -0.618$, $\alpha - \beta = \sqrt5$

$$\frac{x}{1-x-x^2} = \frac{x}{(1-\alpha x)(1-\beta x)} = \frac{1}{\sqrt5}\left(\frac{1}{1-\alpha x} - \frac{1}{1-\beta x}\right) = \frac{1}{\sqrt5}\left(\sum_{n=0}^{\infty}\alpha^n x^n - \sum_{n=0}^{\infty}\beta^n x^n\right) = \frac{1}{\sqrt5}\sum_{n=0}^{\infty}(\alpha^n - \beta^n)x^n = \sum_{n=0}^{\infty}F_n x^n = x + x^2 + 2x^3 + 3x^4 + 5x^5 + \cdots$$

where $F_n = \frac{\alpha^n - \beta^n}{\sqrt5}$

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

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

$\frac{F_{n+1}}{F_n} \to \alpha$ $\quad F_n \sim \frac{1}{\sqrt5}\cdot\alpha^n$ $\quad F_n = \frac{\alpha^n}{\sqrt5}$ 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.

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

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

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

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

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

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

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

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

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

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

$fg = (a_0b_0,\ a_0b_1 + a_1b_0,\ a_0b_2 + a_1b_1 + a_2b_0,\ a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0, \cdots)$ $\quad fg = (c_0, c_1, c_2, c_3, \ldots)$, $c_n = \sum_{k=0}^{n} a_k b_{n-k}$

multiplication is by convolution (not entrywise)

$F[[x]]$ = 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. $F = \mathbb{F}_2 = \{0,1\}$

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

$$x^2+x^4+x^5+x^7+\cdots = (x^5+x^6+x^9+x^{11}+\cdots)(x^{-3}+x^{-2}+1+\boxed{}x^2\cdots)$$

$1x^{-2}$ $0x^{-1}$ $x^0=1$ $0x$ $0x^2$

In the ring $F[[x]]$, the units (ie. invertible elements) are all the elements with nonzero constant term.
$F((x))$ is however a field i.e. all nonzero elements are units
why can't we allow infinitely many powers of x with negative exponents as well as positive exponents?

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

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

$$\underset{\in F(x)}{\frac{1}{x^2+x^3}} = \frac{1}{x^2(1+x)} = \frac{1}{x^2}(1-x+x^2-x^3+x^4-x^5+\cdots) = x^{-2}-x^{-1}+1-x+x^2-x^3+x^4-x^5+\cdots$$

$$\begin{tikzcd}
 & F((x)) \arrow[dl, no head] \arrow[dr, no head] & \\
F[[x]] \arrow[dr, no head] & & F(x) \arrow[dl, no head] \\
 & F[x] \arrow[d, no head] & \\
 & F &
\end{tikzcd}$$

Automorphisms of $\mathbb{Q}(x) \supset \mathbb{Q}$ includes $f(x) \mapsto f(x+1)$ has inverse $f(x) \mapsto f(x-1)$.

$$f(x)+g(x) \longmapsto f(x+1) + g(x+1)$$
$$f(x)g(x) \longmapsto f(x+1)\,g(x+1)$$

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

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 $x \in \mathbb{Q}[\sqrt{x}]$.

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

$$\sqrt{1+x} = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots, \quad a_i \in \mathbb{Q}$$
$$\in \mathbb{Q}[[x]]$$

$$1+x = (a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots)^2 = a_0^2 + 2a_0a_1 x + (a_1^2 + 2a_0a_2)x^2 + (2a_0a_3 + 2a_1a_2)x^3 + (a_2^2 + 2a_1a_3 + 2a_0a_4)x^4 + \cdots$$

$a_0 = \pm 1$. Let's take $a_0 = 1$.

$$= 1 + 2a_1 x + (a_1^2 + 2a_2)x + (2a_3 + 2a_1a_2)x^3 + (a_2^2 + 2a_1a_3 + 2a_4)x^4 + \cdots$$

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

Now $a_1 = \frac{1}{2}$.

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

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

etc.

$$\sqrt{1+x} = 1 + \tfrac{1}{2}x - \tfrac{1}{8}x^2 + \tfrac{1}{16}x^3 - \cdots$$

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

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

$\binom{a}{k} = \dfrac{a(a-1)(a-2)\cdots(a-k+1)}{\underbrace{k(k-1)(k-2)\cdots 2\cdot 1}_{k!}}$. $k\in\{0,1,2,\dots\}$, $a\in\mathbb{R}$.

(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).

$\sqrt{1+x} =$

$$(1+x)^{\frac12} = \underbrace{1}_{\binom{1/2}{0}} + \underbrace{\frac{\frac12}{1}}_{\binom{1/2}{1}}x + \underbrace{\frac{\frac12(\frac12-1)}{2\cdot1}}_{\binom{1/2}{2}}x^2 + \underbrace{\frac{\frac12(\frac12-1)(\frac12-2)}{3\cdot2\cdot1}}_{\binom{1/2}{3}}x^3 + \underbrace{\frac{\frac12(\frac12-1)(\frac12-2)(\frac12-3)}{4\cdot3\cdot2\cdot1}}_{\binom{1/2}{4}}x^4+\cdots$$

$-\frac58\cdot\frac1{16} = -\frac{5}{128}$

$$= 1+\tfrac12 x - \tfrac18 x^2 + \tfrac1{16}x^3 - \tfrac{5}{128}x^4+\cdots \in \mathbb{Q}[[x]]$$

$\sqrt{2+x} = \underbrace{\sqrt2}_{\notin\,\mathbb{Q}}\;\underbrace{\sqrt{1+\tfrac{x}{2}}}_{\in\,\mathbb{Q}[[x]]} \in \mathbb{R}[[x]]$, $\notin \mathbb{Q}[[x]]$

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 $F = \mathbb{F}_q$.

First suppose q is odd i.e. $p=\operatorname{char} F$ is odd.

Half the nonzero elements are squares.

"ABLE WAS I ERE I SAW ELBA"

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

a	a^2
0	0
1	1
2	4
3	2
$-3=4$	2
$-2=5$	4
$-1=6$	1

a	a^2
0	0
±1	1
±2	4
±3	2

$\mathbb{F}_{49} = \mathbb{F}_7[\sqrt3] = \mathbb{F}_7[\sqrt5] = \mathbb{F}_7[\sqrt6] = \mathbb{F}_7[i]$, $i=\sqrt{-1}$

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

x^2-a is irreducible iff $F[\sqrt a]\supset F$ 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 $\mathbb{F}_q$.

$\mathbb{Q}\subset\mathbb{R}\subset\mathbb{R}^*$ $\mathbb{R}$: reals, $\mathbb{R}^*$: hyperreals

Back to basics:

Let R be an integral domain i.e. commutative ring with identity & having no zero divisors (i.e. $a,b\neq 0 \Rightarrow ab\neq 0$)
eg. $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$. An ideal in R is a subset (actually subring) which is closed under taking R-linear combinations. A subset $A\subseteq R$ with $0\in A$ is an ideal if

$$r_1a_1+r_2a_2+\dots+r_ka_k\in A \quad \text{for all } a_1,\dots,a_k\in A;\ r_1,\dots,r_k\in R.$$

Eg. if we fix $a_1,\dots,a_n\in R$ then the ideal generated by $a_1,\dots,a_n$ is

$$(a_1,\dots,a_n)=\{r_1a_1+\dots+r_na_n : r_1,\dots,r_n\in R\}$$

(Compare: the span of a set of vectors in a vector space is a subspace).

Eg. in $\mathbb{Z}$, fix an integer m. The principal ideal generated by m is
$(m)=\{rm : r\in\mathbb{Z}\}=\{\dots,-2m,-m,0,m,2m,3m,\dots\}$ is an ideal in $\mathbb{Z}$.

The quotient ring is $\mathbb{Z}/(m)=\mathbb{Z}/m\mathbb{Z}=\{\text{cosets of } (m) \text{ in } \mathbb{Z}\}=\{(m),1+(m),2+(m),\dots,m-1+(m)\}$

Informally $\mathbb{Z}/m\mathbb{Z}=\{\bar{0},\bar{1},\bar{2},\dots,\overline{m-1}\}$ or more informally $\{0,1,2,\dots,m-1\}$

$\mathbb{Z}/(p)$ is a field. $\mathbb{Z}/(m)$ is not a prime unless m is prime.

$\mathbb{Z}/(6)=\{\bar{0},\bar{1},\dots,\bar{5}\}$ is not a field. $\bar{2}\cdot\bar{3}=\bar{6}=\bar{0}$ (zero divisors $\bar{2},\bar{3},\bar{4}$; units $\bar{1},\bar{5}=-\bar{1}$).

$\mathbb{Z}/(6)$ fails to be a field because the ideal (6) is not maximal; it is contained in (2) and (3).

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Z} \arrow[dl, dash] \arrow[dr, dash] & \\
(2)=\{\dots,-4,-2,0,2,4,6,\dots\} \arrow[dr, dash] & & (3)=\{\dots,-6,-3,0,3,6,9,\dots\} \arrow[dl, dash] \\
 & (6)=\{\dots,-12,-6,0,6,12,18,\dots\} &
\end{tikzcd}$$

$\mathbb{Z}/(2)=\mathbb{F}_2$ and $\mathbb{Z}/(3)=\mathbb{F}_3$ are fields.

examples of maximal ideals (not contained in any larger ideals)

an ideal which is not maximal (it's contained in larger ideals).

The quotient ring R/A is a field iff the ideal A is maximal.

We use this to construct $\mathbb{R}$, $\mathbb{R}^*$ and essentially all other fields.

eg. $\mathbb{Z}[x]$ has many examples of subrings and ideals.

eg. $(x^2+1) \subset \mathbb{Z}[x]$ $\quad (x^2+1) = \{h(x)(x^2+1) \;:\; h(x) \in \mathbb{Z}[x]\}$

$$\mathbb{Z}[x]/(x^2+1) = \{a+bx+\cancel{(x^2+1)} \;:\; a,b \in \mathbb{Z}\} \cong \{a+bi \;:\; a,b \in \mathbb{Z}\} = \mathbb{Z}[i].$$

"Gaussian integers"

Not a field.

The only units (invertible elements) are $1, -1, i, -i$

The ideal (x^2+1) is not maximal.

We have a homomorphism $\phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[i]$

which is onto. Its kernel $f(x) \longmapsto f(i)$ (evaluate at i)

is $\ker \phi = (x^2+1)$.

The first isomorphism theorem for rings: $\underbrace{\mathbb{Z}[x]}_{\text{domain of } \phi} / \underbrace{(x^2+1)}_{\text{kernel of } \phi} \cong \underbrace{\mathbb{Z}[i]}_{\text{image of } \phi}$

$(3) = \{3h(x) : h(x) \in \mathbb{Z}[x]\}$ is also an ideal of $\mathbb{Z}[x]$.

$\mathbb{Z}[x]/(3) \cong \mathbb{F}_3[x]$, $\quad \mathbb{F}_3 = \{0,1,2\}$ $\quad \mathbb{F}_3[x]$ is a ring but not a field. (3) is not a maximal ideal.

$\mathbb{Z}[x]/(3, x^2+1) \cong \mathbb{F}_9 = \{a+bi : a,b \in \mathbb{F}_3\}$.

is a field

$$\begin{array}{ccc} & \mathbb{Z}[x] & \\ & | & \\ & (3, x^2+1) & \\ / & & \backslash \\ (3) & & (x^2+1) \end{array}$$

$(3, x^2+1) = \{3h(x) + (x^2+1)g(x) \;:\; h(x), g(x) \in \mathbb{Z}[x]\}$.

non-maximal ideals

Construction of $\mathbb{R}$ from $\mathbb{Q}$ (one way)

$\mathbb{Q}^\infty = \{(a_0, a_1, a_2, \cdots) : a_i \in \mathbb{Q}\}$ is a ring with coordinatewise addition, multiplication, subtraction

commutative ring with identity

$(1,1,1,1,\cdots)(a_0,a_1,a_2,\cdots) = (a_0, a_1, a_2, a_3, \cdots)$

$(1,0,1,0,1,0,\cdots)(0,1,0,1,0,1,\cdots) = (0,0,0,0,0,0,\cdots) = 0$ zero divisors. $\mathbb{Q}^\infty$ is not a field.

$Z = \{(z_0, z_1, z_2, \cdots) \in \mathbb{Q}^\infty :$ for all n there exists M such that $\underbrace{-\frac{1}{n} < z_k < \frac{1}{n}}_{|z_k| < \frac{1}{n}}$ whenever $k > M\}$.

i.e. $z_k \to 0$ as $k \to \infty$. (The sequence of rationals having $\lim_{k\to\infty} z_k = 0$)

This is a subring $Z \subset \mathbb{Q}^\infty$.

A larger subring $R \subset \mathbb{Q}^\infty$ is the subring of Cauchy sequences i.e.

$R = \{r = (r_0, r_1, r_2, \cdots) \in \mathbb{Q}^\infty$ such that for all n there exists M such that $|r_k - r_l| < \frac{1}{n}$ whenever $k, l > M\}$.

$R \subset \mathbb{Q}^\infty$ is also a subring. (commutative ring with identity)

$Z \subset R$ is a subring, in fact Z is an ideal in R

$R/Z \cong \mathbb{R}$

There is a field extension $\mathbb{R}^* \supset \mathbb{R}$ having infinitesimals and infinite elements.

In $\mathbb{R}^*$ there exist elements $\varepsilon \in \mathbb{R}^*$ such that $\varepsilon > 0$ but $\varepsilon < \frac{1}{n}$ for $n = 1, 2, 3, \cdots$

Note: $Z \subset \mathbb{Q}^\infty$ is not an ideal in $\mathbb{Q}^\infty$ e.g. $\underset{\uparrow\, Z}{(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \cdots)} \cdot \underset{\uparrow\, \mathbb{Q}^\infty}{(1,2,3,4,5,\cdots)} = \underset{\not\uparrow\, Z}{(1,1,1,1,1,\cdots)}$

$\mathbb{R}^\infty = \{(r_0, r_1, r_2, r_3, \dots) : r_i \in \mathbb{R}\}$ commutative ring with identity $1 = (1, 1, 1, \dots)$

We will construct $\mathbb{R}^* = \mathbb{R}^\infty / Z$ where $Z \subset \mathbb{R}^\infty$ is a maximal ideal. What max. ideal is this?

$= \{(0, *, 0, *, *)\}$

$\mathbb{R}^5 = \{(r_0, r_1, r_2, r_3, r_4) : r_i \in \mathbb{R}\}$ has 32 ideals e.g. $J = \{(0, r_1, 0, r_3, r_4) : r_1, r_3, r_4 \in \mathbb{R}\}$

$U = \{(r_0, r_1, r_2, r_3, r_4) : r_0 + r_1 + r_2 + r_3 + r_4 = 0\}$ is a subspace of $\mathbb{R}^5$ but not an ideal e.g.

$$\underset{\mathbb{R}^5}{\underset{\cap}{(5,0,0,0,0)}} \cdot \underset{U}{\underset{\uparrow}{(1,1,1,1,-4)}} = (5,0,0,0,0) \notin U$$

$\mathbb{R}^5 / J \cong \mathbb{R}^2$

$\mathbb{R}^5 / \{(0, *, *, *, *)\} \cong \mathbb{R}$

Nothing new.

$\{(*,*,*,*,*)\} = \mathbb{R}^5$

$\{(*,*,*,*,0)\}$ . . . $\{(0,*,*,*,*)\}$ 5 maximal ideals

$\{(*,*,0,0,0)\}$

$\{(*,0,0,0,0)\}$ $\{(0,*,0,0,0)\}$ . . . $\{(0,0,0,0,*)\}$

$\{(0,0,0,0,0)\}$

$\mathbb{R}^\infty = \{(*****\cdots)\} = \{(r_0, r_1, r_2, r_3, \cdots) : r_i \in \mathbb{R}\}$ comm. ring with identity

$J = (0*****\cdots) = \{(0, r_1, r_2, r_3, r_4, \cdots) : r_i \in \mathbb{R}\}$

$\mathbb{R}^\infty / J \cong \mathbb{R}$ (Boring)

$\overset{u}{(1,0,1,0,1,0,\cdots)}\overset{v}{(0,1,0,1,0,1,\cdots)} = (0,0,0,0,0,0,\cdots)$

If we pick an ideal Z containing both u and v then $u+v \in Z$ i.e. $1 = (1,1,1,1,\cdots) \in Z$

but then $x \cdot 1 = x \in Z$ for all $x \in \mathbb{R}^\infty$, $\mathbb{R}^\infty/Z = \mathbb{R}^\infty/\mathbb{R}^\infty = 0$

Among all ideals in $\mathbb{R}^\infty$ we must choose Z as large as possible but $Z \subset \mathbb{R}^\infty$ (proper subset)

i.e. $1 \notin Z$. Z has no units (no invertible elements)

Z must contain either u or v but not both.

If $u, v \notin Z$ then pick one, say u, $Z + \underbrace{\mathbb{R}^\infty u}_{\text{multiples of } u} \supset Z$ is a larger ideal without containing 1.

$\underset{\hat{Z}}{(1,0,0,0,0,\cdots)} + \underset{\hat{Z}}{(0,1,1,1,1,\cdots)} = \underset{\hat{Z}}{(1,1,1,1,1,\cdots)}$

$\mathbb{R}^* \supset \mathbb{R}$. Every $a \in \mathbb{R}$ is identified as $(a,a,a,a,\cdots)$

eg. $\varepsilon = (1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \cdots) \in \mathbb{R}^\infty$ is infinitesmal.

$0 < \varepsilon < 0.01$ because

$(1,0,0,1,0,0,1,0,0,\cdots)(0,1,1,0,1,1,0,1,1,\cdots) = (0,0,0,0,\cdots)$

$\varepsilon \cdot \underbrace{(1,2,3,4,5,\cdots)}_{(2,3,4,5,6,\cdots)} = (1,1,1,1,\cdots) = 1$