Fields

Book III

We have been folking about number fields: finite extensions $E \supseteq Q$ i.e. $(E:Q) = n < \infty$. (Some are Galois :e. $G = Aut E$ satisfies $ G = n$; but in general $ G \leq n$.)
Back to bassis: In a field F, if 1+1+1++1=0 then the smallest a for which this occurs is the characteristic of F
n ≥1
If F has characteristic $n > 0$ then n must be prime. If $n = ab$, $a, b \ge 1$ then $(1+1+\dots+1)(1+1+\dots+1) = 1+1+1+\dots+1 = 0$ n = ab
By minimality of n, n is prime. If 1+1++1 =0 for any n>1, then we say n has characteristic 0.
Given a field F, char F = characteristic of F is either 0 or p (some prime p). If char F = p then F \supseteq H = field of order p ($\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-i\} = $ "integers wood p "). eg. H = \mathbb{F}_p , \mathbb{F}_p , \mathbb{F}_p , \dots , $\mathbb{F}_p(\pi) = \{ell inclinal functions in \pi with coefficients in \mathbb{F}_p\},$
g. IF, IF, IF, IF,, IF, (N)= & all rational functions in x with coefficients in IF,
■ If char F= 0 then F = Q. Eg. R, C, Q, number fields, A = Salgebraic numbers 3 C C eg. QUEI
In either case F has a unique smellest subfield, either F or Q, called the prime subfield of F.

_

_

All fields of characteristic O are infinite. (They are extensions	of Q, hence vector sprces are Q.)
IF EZF is a field extension (i.e. E. Fase fields with	Fa subfield of E) then
All fields of characteristic D are infinite. (They are extensions IF E 2 F is a field extension (i.e. E, F are fields with E is a vector space over F. The dimension of this vector	r space is the degree [E:+] of
this extension eg_	
	ອີໂອ. ຕີ 1
4. 2.1	
21,13 60315 1, VZ, V3, J5, V6, J7, V0, J17, 2 are (in. indep.	2 🛇
are (in malep.	
T P. O. D of the D of a con fits and	ace fraite
For fields of characteristic a prime p , some ave finite, some a Given p prime and $k \ge 1$ (positive integer), there is a unique	Rild of order q= pk (up to isomorphism
Given p prime and k = 1 (positive integer), (mede 15 à 77	
Finite fields: It,	
$F_{q} = \{0, 1, \alpha, \beta\} + 0 \alpha \beta$ $= \{0, 1, \alpha, \beta\} + 0 \alpha \beta$ $= 0 \alpha \beta$	$char F_{a} = 2$.
14 - 10, 14, 13	
	$\mathbb{F}_{4} \supset \mathbb{F}_{2}$ of degree $[\mathbb{F}_{4} : \mathbb{F}_{2}] = 2$
d ox R 1	with basis 1, x
	$F_q = \{a_1 + ba : a_i b \in F_2\}$
PIP & Top & PIP & Top &	
$\alpha' + \alpha = (1 + i)\alpha = 0\alpha = 0$	= $\{0, 1, \alpha, 1+\alpha\}$ where $\alpha = \alpha+1$.
	$= \{0, 1, u, a\}$ β
	$\int_{\mathcal{A}} \int_{\mathcal{A}} \int$
	The minimal poly. of & over the is x + x+ s
	· · · · · · · · · · · · · · · · · · ·

Irreducible polynomials over IF. = {0,13 There are 2" polynomials of degree n: x"+ cn, x"+ ...+ Cr and they are all mornic, Co, C1, ..., Ca-i E Fz $x^{2} + c_{x}x^{2} + \cdots + c_{x}x + c_{0}$ dagues 1: X, X+1 (both irreducible) degree 2: x^{2} , $x^{2}+1$, $x^{2}+\pi$, $x^{2}+\pi+1$ $x \cdot x$ $(\pi+1)(\pi+1)$ $x(\pi+1)$ irreducible Let α be a nost of $x^2 + x + 1$. The other noof is $\alpha + 1$. $\alpha^2 + \alpha + 1 = 0 = 7 \quad \alpha^2 = -\alpha - 1 = K + 1$ reducible Note: The rests of an2+6x+C=0 are -b±15-me except in characteristic 2. hegree 3: x3 = X.X.X $x^{3}+1 = (x+1)(x^{2}+x+1)$ $x^3+x = x \cdot (x+i)^2$ x + X+1 irreducible ie. Y= 1+1 F= Fa[8] where I is a not of x3+x+1 $\chi^{3}_{+}\chi^{2} = \chi \cdot \chi \cdot (\chi + i)$ $\chi^{3}_{+}\chi^{2}_{+/}$ irreducible $= \{a, l+b, q+c, q^2 : a, b, c \in \mathbb{R}\}.$ $\gamma = 1$ $x^{2} + x^{2} + x = x(x^{2} + x + i)$ = {0,1,1, 1+1, 8, 8+1, 9+9, 1+9+13. $q' = \gamma + \cdots + \gamma$ $x^{2} + x^{2} + x + 1 = (x + 1)^{3}$ 76 94 75 $\gamma = \gamma^{-}$ In general the nonzero daments of Fa form a cyclic group of order q-1. $q_{=}^{3} = q_{+}^{3} + 1$ $x^3 + x + 1$ has three roots in f_8 : $\gamma, \gamma^2, \gamma^4$. $q^{\dagger} = \gamma^{\dagger} + \gamma^{\dagger}$ 95= 13+92 = 9+9+1 X+x2+1 has three works in Its: $\gamma^{b} = \gamma^{2} + \gamma^{2} + \gamma = (1+1) + \gamma + \gamma$ There is only one finite field of each order q=pt (p prime, k>1) up to isomorphism $\mathbf{T}^{\mathbf{s}}, \mathbf{T}^{\mathbf{s}}, \mathbf{T}^{\mathbf{s}} = \mathbf{T}^{\mathbf{s}}, \mathbf{T}^{\mathbf{s}} = \mathbf{T}^{\mathbf{s}}$ $\gamma^{7} = \gamma^{5} + \gamma = (\gamma^{4}) + \gamma^{2} = (\gamma^{4})$ If \mathbb{F}_q is a finite field then it must have cher $\mathbb{F}_q = p$ 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 $\mathbb{F}_q \supseteq \mathbb{F}_p$ $|\mathbb{F}_q| = q < \infty$. Let $\alpha_{i_1} \cdots, \alpha_h$ be a besis for \mathbb{F}_q over \mathbb{F}_p i.e. $\mathbb{F}_q = \{q_i \alpha_i + q_i \alpha_h : q_i, \dots, q_k \in \mathbb{F}_p\}$. $g = \left(\left| f_{g} \right| \right) = p^{n} p^{n} + p^{n}$

$F_q = F_s[i]$ compare : $G = R[i]$,	Q[i] > Q i=J-1. SI, i? is a bassis of the extension Q[JZ] > Q in each case
= $\{a+bi: a, b \in \overline{H_3}\}$ = $\{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$	$i = F_1 = \sqrt{2}$ $H_2 = H_2 [i] = H_2 [J_2]$
$\theta^{\prime \prime} \theta^{\prime \prime} \theta^{\prime$	
Q is a primitive doment: its powers	$\theta^2 = (1+i)^2 = /(1+2i) + j^2 = 2i$
O is a primitive clement: its powers give all the nonzers dements of IFg.	$\theta^{3} = \underbrace{2i}_{\theta^{2}} \underbrace{(i+i)}_{\theta^{2}} = -2 + 2i = 1 + 2i$
	$\theta = \theta^{q} \theta = (1+2i)(1+i) = 1-2 = -1=2$ $\theta^{s} = \theta^{q} \theta = -\theta = 2\theta = 2+2i$
	$\theta^{4} = \theta^{2} \theta = (1+2i)(1+i) = 1-2 = -1=2$ $\theta^{5} = \theta^{4} \theta = -\theta = 2\theta = 2+2i$ $\theta^{6} = \theta^{4} \theta^{2} = -\theta^{2}$ $\theta^{7} = \theta^{4} \theta^{3} = -\theta^{3}$ $\theta^{8} = \theta^{4} \theta^{4} = -\theta^{4}$
Every finite field IFz (q=pk, p prime)	$\theta = 0.0$
has a primitive element i.e. an element whose powers give all the nonzero field element	$\xi = - \frac{1}{2}$
Why? Idea of proof: Eq. to see that It's has primitive element: The nonzero elements for group of order &. There are five groups of	n a multiplicative 5° 67
Komorphism: dihekoal goons of order 8 (symmet	y group of a square) { nonabelian $S=-2$ Levery deliver group is a direct product of cyclic
quaternion	reats, of order 4, Every abdien group is a direct product of cyclic groups
abelicing Cz × Cz (four elements of order 8, for element of Cz × Cz (four elements of order 4, the Cz × Cz × Cz (with series elements of	se claments of order 2) (muttiplicative
1. Cr×Cr×Cr (with series of	order 2) Ca = \$1,9,9,,9, 3, 9=1

In a field of order 9 the polynomial 2-1	has at most 2 roots.		· · · · · · · ·
In a field of order 9, the polynomial $\vec{x}-1$ (In $F[x]$, where f is any field, every If $f(x) \in F[x]$ has k noots $r_1, \dots, r_k \in F$, the $\vec{x}-1 = (x-1)(x+1)$	she nomial of degree & ha	s at most k	roots.)
If f(x) < F[x] has k motor r,, r < F, the	$f(x) = (x-r_{i})(x-r_{2}) - (x-r_{k})h(x)$		
	legner k		
$x^{2}-1 = (x-1)(x+1)$			
$\overline{H_{25}} = \overline{H_{5}}[\overline{J_{2}}] \neq \overline{H_{5}}[\overline{J_{1}}] = \overline{J_{4}} = \pm 2$	In Fis, -1 is dready a spu	are .	
1, 12 is a besis	$H_{s}[i] = H_{s}[2] = H_{s}$		
· · · · · · · · · · · · · · · · · · ·	$Q[\overline{y}\overline{4}] = Q[2] = Q$		
	$R[J\overline{z}] = R$		
	$\mathbb{R}[i] = C$		
In $R[\pi]$, $\chi^2 - 2$ is reducible since $\chi^2 - 2 = (\chi + \sqrt{\epsilon})$	(3~ ^x)		
How do we extend to to the? We want a go	undratic extension [F: F]	-2,	
A choice of basis is \$1, 503 if at I is	not a square of any element	in the i.e. X	$-a \in f[x]$
	On the a life the	Should be me	lf are more
How do we extend F_p to F_p ? We want a que A choice of basis is $S1, Ta 3$ if $a \in F_p$ is When p is an odd prine, there are p-1 nonzero When $p=5$, the nonzero elements of F_5 are 123,4	200 ecembers and here of your	are spranes, a	
When p=5, the nonzero elements of to are 12,3,9	stare 1,4 de squares; 2,	3 are no-squares	2
$H_{\rm L} = H_{\rm L} [H_{\rm L}] = H_{\rm L} [H_{\rm L}]$			
$p_{a} = 2, x^2 = (x_a)^2$ i.e. $x^2 = \pi \cdot \pi$	$x^{2} = (x - b^{2})^{2}$	0,13 has squar	es only.
When $p=2$, $x^2-a = (x-a)^2$ i.e. $x^2 = x \cdot \pi$, reducible	reducible But n27 IT_a = IT_a (x), a	x+1 is irredu	cible in #[x]
	$I_{4} = I_{2} [\alpha] , \alpha$	root of x2+x-	F[1.]

If q=pt then the It is an extension of degree [It It] = k with exactly k automorphisms.
In $H_q = H_z[i]$, the map at bit a -bit is the nonideratity automorphism. In $H_{zz} = H_z[Jz]$, the in $a+bJz \rightarrow a-bJz$.
$ F_4 = F_{\epsilon}[\kappa] \text{the map } i \rightarrow i \cdots \rightarrow i \\ = \{0, i, \alpha, \beta\} \qquad $
Finite fields are Galois extensions of their prime fields: $\mathbb{F}_2 \ge \mathbb{F}_p$, $q = p^k$, p prime $[\mathbb{F}_2:\mathbb{F}_p] = k$ so $G = \operatorname{Aut} \mathbb{F}_q$ has order $ G = k$ and $G = \{1, 0, 0^2, \dots, 0^{k-3}\}$, $\sigma^{k} \ge 1$. Here $\sigma(\pi) = \pi^p$.
$[f_{\overline{q}}: f_{\overline{p}}] = k so G = Aut f_{\overline{q}} has order IG(=k and G = \{L, \sigma, \sigma^2, \dots, \sigma^{k-1}\}, \sigma^k = \iota Here \sigma(\pi) = \pi^p.$
$\sigma(xy) = (xy)^2 = \sigma(x)\sigma(y) \text{for all } x, y \in H_g$
$\sigma(x+y) = (x+y) = x^{p} + px^{p}y + \frac{p(p)}{2}x^{p}y^{2} + \dots + pxy^{p} + y^{p}$ by the Binomial Theorem $(x+y)^{p} = \sum_{k=0}^{\infty} {\binom{n}{k}x^{k}y^{k}}$
$\sigma: H_2 \rightarrow H_2 is a homomorphism All elements of H_2 are noots of H_2 - x. \begin{pmatrix} n \\ i \end{pmatrix} = \frac{n!}{i! (n-i)!} n! = 1 = \begin{pmatrix} n \\ i \end{pmatrix}$ $f_1 = n (n-i) = n (n-$
σ: Hz → Hz is a homomorphism. All elements of Hz are roots of x=x. (2) = 2!(n-2)! 2 Ht. (N)
ker $\sigma = \{x \in F_q : \sigma(x) = o\} = \{o\}$ so σ is one-to-one. $(o) = \overline{\sigma + n} = (u)$
Since Fig is finite, o is onto. So o is an isomorphism to the is an antomorphism of
Aut Tig 2 \$1, 5, 5, 5, 5, 5 but these automorphisms can't all be distinct
$\sigma^{k}(x) = \sigma(\sigma(\sigma(\cdots(\sigma(x))))) = (((a \stackrel{p}{})^{p}))) = \chi^{p} = \chi^{p} = \chi^{p} = \chi^{p}$ In $f_{2} = \{x \in f_{2} : x \neq 0\}$ is a multiplicative group (actually of order $q = i$ $\chi^{p} = i$ for all $\chi \in f_{2}^{*}$

Eq. $\mathbb{F}_{q} > \mathbb{F}_{z}$ of degree $[\mathbb{F}_{q} : \mathbb{F}_{z}] = 2$ with basis $\{1, \alpha\}$	x $\overline{v}(x) = x^2 - \overline{s}(x) = x^4$
$\mathcal{A} = \{\mathcal{A} \mid \mathcal{A} \mid$	
$= \{a \cdot 1 + b \cdot \alpha : a, b \in \mathbb{F}_{2}^{2} \}$ $= \{c, \sigma\}$ $\ z$	β β β.
Eq. $\overline{H_q} \supset \overline{H_q} = \{0, 1, 2\}$, $[\overline{H_q}: \overline{H_q}] = 2$ with basis $\{1, i\}$ $\overline{O(x)} = x^3$	x
$F_q = \{a + bi : a, b \in F_q\}$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$i = \sqrt{-1} = \sqrt{2}$ for $a, b \in \mathbb{R}_{2}$ for $a, b \in \mathbb{R}_{2}$ $f = \langle \sigma \rangle = \{\iota, \sigma\}$	-i=2i $-2i=i$
	attoi 4-bi 3.231.245-11.3
(<i>a</i> +b _i) ⁼	$q^{3} + 3q^{2}b_{1} + 3q(b_{1}) + (b_{1})^{3}$
Eq. $F_g \supset F_2 = \{o, i\}$, $[F_g : F_2] = 3 = G $ where $f = Aut F_g = \langle \sigma \rangle = \{i, \sigma, \sigma^2\}$, σ^2 .	
$F = \{a + b\gamma + c\gamma^2 : a; b; c \in F \{\gamma^3 = \gamma + 1\} \sigma(x) = x^2, \qquad x$	$\sigma(x) = x^2$
$\begin{cases} 1, 1, 1^{2} \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ $	$\frac{1}{\gamma^2}$
	$\begin{array}{c} \gamma t = \gamma + \gamma^2 \\ 1 + \gamma \qquad \gamma t^{b} = 1 + \gamma^2 \end{array}$
$\overset{\circ}{\overset{\circ}{\overset{\circ}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}}{\overset{\circ}}{\overset{\circ}{\overset{\circ}}{\overset{\circ}}{\overset{\circ}}{\overset{\circ}}{\overset{\circ}{\overset{\circ}$	$\begin{array}{cccc} +\gamma & \gamma b_{-} & +\gamma^{2} \\ f_{+}\gamma^{2} & \gamma \\ \tau_{+}(\tau_{+}) & \gamma_{-}^{2} & +\gamma \\ \end{array}$
γ	$2 + 1 + 1^{2}$ $\gamma^{2} = \gamma^{2} + \gamma^{2} + 1$

If $f(x) \in F[x]$ is irreducible, then we say any first roots x, p of $f(x)$ (typically in an extension field $E \supseteq F$) then x, β are conjugates. Eq. $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ has roots $\pm \overline{y} \in R$ or in $\mathbb{Q}[\overline{y}\overline{z}]$. $\pm \overline{y}\overline{z}$ are conjugates. If $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ has roots $\pm \overline{y} \in C$ or $\mathbb{Q}[\overline{z}]$. $\pm i$ are conjugates. In E there can be an anter-orphism $\overline{v} \in Aut E$ fixing every dement of F and mapping a root of $f(x)$ to any of its conjugates. Eq. $f(x) = x^2 - 2$ has three roots x, aw, aw^2 where $w = \sqrt{2}$, $w = e^{2\pi i/3} = -\frac{1+\sqrt{2}}{2}$, $w^2 = e^{\pi i/3} = -\frac{1+\sqrt{2}}{2}$. Eq. $f(x) = x^2 - 2$ has three roots x, aw, aw^2 where $w = \sqrt{2}$, $w = e^{2\pi i/3} = -\frac{1+\sqrt{2}}{2}$, $w^2 = e^{\pi i/3} = -\frac{1+\sqrt{2}}{2}$. The doments $x, ww, wis are an anter-orphism. There are all the conjugates of x.in \mathbb{Q}[x, w] \supset \mathbb{Q}, [\mathbb{Q}[w, w] : \mathbb{Q}] = 6.x^2 = (x - \alpha)(x - \alpha w)(x - \alpha w^2)\mathbb{Q}[w] is not the splitting field of f(x) = x^2 - 2\mathbb{Q}[w] is not the splitting field of f(x) = x^2 - 2[\mathbb{Q}[w] : \mathbb{Q}] = 3[\mathbb{Q}[w] : \mathbb{Q}] = 3[\mathbb{Q}[w] : \mathbb{Q}] = 3[\mathbb{Q}[w] : \mathbb{Q}] = 3[\mathbb{Q}[w] : \mathbb{Q}] = 3\mathbb{Q}[w] then \mathbb{Q}[w].$
Eq. $f(x) = x^{2} \in \mathbb{Q}[x]$ has nots $\pm j_{2} \in \mathbb{R}$ or in $\mathbb{Q}[vz]$. $\pm vz$ are conjugates. If $f(x) = x^{2} + i \in \mathbb{Q}[x]$ has nots $\pm i \in \mathbb{C}$ or $\mathbb{Q}[i]$. $\pm i$ are conjugates. In E there can be an automorphism $v \in Aut E$ fixing every element of F and mapping a not of $f(x)$ to any of its conjugates. Eq. $f(x) = x^{2} - 2$ has three noots x , and and $v = \sqrt[3]{2}$, $w = e^{2\pi i/3} = -\frac{1+\sqrt{3}}{2}$, $w = e^{\frac{\pi}{2}} -\frac{1-\sqrt{3}}{2}$. The elements x , and $v = conjugates$. In $\mathbb{Q}[x, w] \supset \mathbb{Q}$, $[\mathbb{Q}[x, w] : \mathbb{Q}] = 6$ $x^{2} - (x-\alpha)(x-\alpha w)(x-\alpha w^{2})$ $\mathbb{Q}[x]$ is not the splitting field of $f(x) = x^{2} - 2$ $\mathbb{Q}[x]$ is not the splitting field of $f(x) = x^{2} - 2$ $\mathbb{Q}[x] = 3$ $\mathbb{Q}[y] \mathbb{Q}[ww] \mathbb{Q}[ww]$
If $g(x) = x^{2} + i \in Q[x]$ bes voits $\pm i \in C$ or $Q[i]$. $\pm i$ are conjugates In E there can be an automorphism of that E fixing every dement of F and mapping a root of $g(x)$ to any of its conjugates. Eq. $f(x) = x^{2} - 2$ has there roots x , and, and index $\alpha = 3\sqrt{2}$, $\omega = e^{2\pi i/3} = -\frac{1+\sqrt{2}}{2}$
In E there can be an automorphism of Aut E fixing every dement of F and mapping a root of $f(x)$ to any of its conjugates. Eq. $f(x) = x^{2} = 2$ has three roots x , dw , dw^{2} where $w = \sqrt{2}$, $w = e^{2\pi i/3} = -\frac{1+\sqrt{2}}{2}$, $w^{2} = e^{2\pi i/3} = -\frac{1+\sqrt{2}}{2}$. The elements x , wo , w^{2} are conjugates. There are all the conjugates of x . in $\mathbb{Q}[x,w] \supset \mathbb{Q}$, $[\mathbb{Q}[x,w]:\mathbb{Q}] = 6$ $x^{2} - 2 = (x-\alpha)(x^{2}-\alpha w)(x-\alpha w)(x-\alpha w)$ $\mathbb{Q}[x,w]$ is the splitting field of $f(x) = x^{2} - 2$ $\mathbb{Q}[x]$ is not the splitting field of $f(x) = x^{2} - 2 = (x-\alpha)(x^{2}+\alpha x + \alpha^{2})$ $[\mathbb{Q}[x]:\mathbb{Q}] = 3$ $[\mathbb{Q}[x]:\mathbb{Q}] = 3$ $\mathbb{Q}[n]$ $\mathbb{Q}[nw]$: $\mathbb{Q}] = 3$
Eq. $f(x) = x^{2} = 2$ has these roots x, aw , aw and $x = y^{2}$, $w = x^{2}$. The elements x, w , w^{3} are conjugates. These are all the conjugates of x . in $\mathbb{Q}[x, w] \supset \mathbb{Q}$, $[\mathbb{Q}[x, w] : \mathbb{Q}] = 6$ $x^{2} = (x-\alpha)(x-\alpha w)(x-\alpha w^{2})$ $\mathbb{Q}[x, w]$ is the splitting field of $f(x) = x^{2} - 2$ $\mathbb{Q}[x]$ is not the splitting field of $f(x) = x^{2} - 2 = (x-\alpha)(x^{2} + \alpha x + \alpha^{2})$ $\mathbb{Q}[x]$ is not the splitting field of $f(x) = x^{2} - 2 = (x-\alpha)(x^{2} + \alpha x + \alpha^{2})$ $\mathbb{Q}[x] : \mathbb{Q}] = 3$ $\mathbb{Q}[x, w]$ $\mathbb{Q}[x] : \mathbb{Q}] = 3$ $\mathbb{Q}[x] : \mathbb{Q}] = 3$ $\mathbb{Q}[x] = 3$ \mathbb
Eq. $f(x) = x^{2} = 2$ has these roots x, aw , aw and $x = y^{2}$, $w = x^{2}$. The elements x, w , w^{3} are conjugates. These are all the conjugates of x . in $\mathbb{Q}[x, w] \supset \mathbb{Q}$, $[\mathbb{Q}[x, w] : \mathbb{Q}] = 6$ $x^{2} = (x-\alpha)(x-\alpha w)(x-\alpha w^{2})$ $\mathbb{Q}[x, w]$ is the splitting field of $f(x) = x^{2} - 2$ $\mathbb{Q}[x]$ is not the splitting field of $f(x) = x^{2} - 2 = (x-\alpha)(x^{2} + \alpha x + \alpha^{2})$ $\mathbb{Q}[x]$ is not the splitting field of $f(x) = x^{2} - 2 = (x-\alpha)(x^{2} + \alpha x + \alpha^{2})$ $\mathbb{Q}[x] : \mathbb{Q}] = 3$ $\mathbb{Q}[x, w]$ $\mathbb{Q}[x] : \mathbb{Q}] = 3$ $\mathbb{Q}[x] : \mathbb{Q}] = 3$ $\mathbb{Q}[x] = 3$ \mathbb
in $Q[\alpha, \omega] \rightarrow Q[\alpha, \omega]$ $\chi^{2}-2 = (\pi - \alpha)(\pi - \alpha\omega^{2})$ $Q[\alpha, \omega]$ is the splitting field of $f(x) = \pi^{2}-2$ $Q[\alpha]$ is not the splitting field of $f(x) = \pi^{2}-2 = (\pi - \alpha)(\pi^{2} + \alpha x + \alpha^{2})$ $[Q[\alpha]]$ is not the splitting field of $f(x) = \pi^{2}-2 = (\pi - \alpha)(\pi^{2} + \alpha x + \alpha^{2})$ $[Q[\alpha]] : Q] = 3$ $[Q[\alpha, \omega] \rightarrow 2/21$ $[Q[\alpha, \omega] \rightarrow 2/21]$
in $Q[\alpha, \omega] \rightarrow Q[\alpha, \omega]$ $\chi^{2}-2 = (\pi - \alpha)(\pi - \alpha\omega^{2})$ $Q[\alpha, \omega]$ is the splitting field of $f(x) = \pi^{2}-2$ $Q[\alpha]$ is not the splitting field of $f(x) = \pi^{2}-2 = (\pi - \alpha)(\pi^{2} + \alpha x + \alpha^{2})$ $[Q[\alpha]]$ is not the splitting field of $f(x) = \pi^{2}-2 = (\pi - \alpha)(\pi^{2} + \alpha x + \alpha^{2})$ $[Q[\alpha]] : Q] = 3$ $[Q[\alpha, \omega] \rightarrow 2/21$ $[Q[\alpha, \omega] \rightarrow 2/21]$
$x^{2}-2 = (x-\alpha)(x-\alpha\omega)(x-\alpha\omega^{2})$ $R[\alpha,\omega] is the splitting field of f(x) = x^{2}-2 = (x-\alpha)(x^{2}+\alpha x + \alpha^{2}) R[\alpha] is not the splitting field of f(x) = x^{2}-2 = (x-\alpha)(x^{2}+\alpha x + \alpha^{2}) \left[\Omega[\alpha] is not the splitting field of f(x) = x^{2}-2 = (x-\alpha)(x^{2}+\alpha x + \alpha^{2}) \left[\Omega[\alpha] is not the splitting field of f(x) = x^{2}-2 = (x-\alpha)(x^{2}+\alpha x + \alpha^{2}) \left[\Omega[\alpha] is not the splitting field of f(x) = x^{2}-2 = (x-\alpha)(x^{2}+\alpha x + \alpha^{2}) \left[\Omega[\alpha] is not the splitting field of f(x) = x^{2}-2 = (x-\alpha)(x^{2}+\alpha x + \alpha^{2}) \left[\Omega[\alpha] is not the splitting field of f(x) = x^{2}-2 = (x-\alpha)(x^{2}+\alpha x + \alpha^{2})$
$Q[\alpha, \omega]$ is the splitting field of $f(x) = x^2 - 2$ $Q[\alpha]$ is not the splitting field of $f(x) = x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$ $[Q[\alpha] : Q] = 3$ $Q[\alpha, \omega]$ $Q[\alpha, \omega]$
Q[a] is not the splitting field of $f(x) = x^2 - 2 = (x - \alpha)(x + \alpha x + \alpha)$ $\begin{bmatrix} Q[a] : Q] = 3 \qquad \qquad$
Q[a] is not the splitting field of $f(x) = x^2 - 2 = (x - \alpha)(x + \alpha x + \alpha)$ $\begin{bmatrix} Q[a] : Q] = 3 \qquad \qquad$
$ \begin{bmatrix} Q[v] : Q] = 3 \\ Q[v] : Q] = 2 \\ \begin{bmatrix} Q[v] \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ $
$\begin{bmatrix} 0 & 1 \\ 0 \end{bmatrix} = 2$
$\begin{bmatrix} \mathbb{Q} \left[\left(\mathbf{w} \omega \right) : \mathbb{Q} \right] = 3 \qquad \qquad$
R Z

Eq. $H_g \supset F_z = \{o, i\}$, $[H_g : F_z] = 3 = G $ where $f = \operatorname{Aut} F_g = \langle \sigma \rangle = \{i, \sigma, i\}$ $H_g = \{a + b\gamma + c\gamma^2 : a, b, c \in H_z\}$, $\gamma^3 = \gamma + 1$ $\{1, 1, \gamma^2\}$ basis $H_g = \{a + b\gamma + c\gamma^2 : a, b, c \in H_z\}$, $\gamma^3 = \gamma + 1$ $\sigma^2(x) = (x^2)^{\frac{1}{2}} = x^4$ $\sigma^2(x) = (x^2)^{\frac{1}{2}} = x^3 = x$			
$\begin{cases} 1, 1, 1^{2} \\ 3 \\ F \\ 1 \\ F \\ 1 \\ F \\ 1 \\ 1 \\ 1 \\ 1 \\ 1$		$ \begin{array}{c} 1 = 1 + 1 \\ 76 = 1 + 7^{2} \\ 1 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 7 \\ 1 \\ 1 \\ 1 \\ 7 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1$	••••
$f(x) = x^3 + x + 1 \in H_2(x)$ is inveducible It has roots in H_g : $\gamma, \gamma^2, \gamma^4$		<u>.</u>	~ ¹⁰ 2
$f(x) = x^{3} + \pi + i = (x - \tau)(x - \tau^{2})(\pi - \tau^{4})$ $(\tau^{3} + \tau + i) = 0$	t(13)=1	$ \begin{array}{c} \mathbf{y} \\ \mathbf{y} \\ \mathbf{y} \\ \mathbf{y}^{12} = \mathbf{y}^{5} \end{array} $	V-7
$7^{\circ} + 7^{\circ} + 1 = 0$ $7^{\circ} + 7^{\circ} + 1 = 0$ $7^{\circ} \in \overline{H_g}$ must have minimal poly. $g(x) \in \overline{F_s}(\pi)$ of daysee 3. This must be so $g(x) = \pi^3 + \chi^2 + 1$ must have roots $7^{\circ}, 8^{\circ}, 7^{\circ}$ $7^{\circ} = 10^{\circ}$ 8 $\overline{10}$ 0 0 0 $\overline{10}$ of t ob a b	$g(x) = x^3 + y$	¢+)	· ·
The roots of x-x E F_(x) are all the eight elements of			•••
$\chi^{\mathcal{B}}_{-\chi} = \chi(\chi^{\mathcal{P}}_{-1}) = \chi(x_{-1})(\chi^{6} + \chi^{5} + \chi^{4} + \chi^{3} + \chi^{2} + \chi + 1)$ = $\chi(x_{+1})(\chi^{3} + \chi + 1)(\chi^{3} + \chi^{2} + 1)$ 0 $\chi^{\mathcal{B}}_{-\chi}(\chi^{2}) = \chi^{\mathcal{B}}_{-\chi}(\chi^{2})(\chi^{3} + \chi^{2}) + \chi^{2}$			· · ·

•	•	#5	5	•	• 4		. (me	nt.	5 -		2		00	5	ъ	?	- X 		x .	2 .	- X 	(x ¹	- 7)) <u>-</u> - - -	· · ·	×6	2 4 -		(x-	-1) -1) 	M	= -	() 7 0	(-2 (x-)() -1) 1	r−3)(x)() -2 2	x)() (x-3 ?	×+ / 5) (5) Gr- 4	-9) 7	•	•	•	•	•	•	
•	S	ub	fi	de	ls	. 2	f	1	- 16	:	Ę		Æ		Fr.		•	•	•	•	•	•	•	•	•	•	•	5	58	· ·	2]	14	3	• •		•	•	•	•	•			用ノ	1016		•	•	•	•	•	
•	•	•	•	•	•	•	•	· ·		110	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	· ·	•	•	•	• •		•	•	•	IF,) 				2	4 F	•	•	•	•	•	
•	•	•	•	•	•	•	•	• •			• .	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	• •	•	•	•			•	•	•	2	L.	/ !\		/:	3	" '8		•	•	•	•	
										F2																															. F	2					•				
•	•		i E. D	0		· ~~			1	-		0		- '.		د.		_	AP.				0		1 1	4	-														•										
•	•	M Pi	at nti	h na	4 m	55 Ę	o Sa	2 2	3pr f	-in 20'	8- 24 21	20	725 m	5 - 2	= * De	45 ^ع د `	7		(lu 8:	eo : 30 Put	8 Da	n. Ma	₹ 	トイン	ru : 3	nk op	ver m	s ject	: : : :	line	•••	•	•	• •	· · ·	•	•	•	•	•	•			•	•	•	•	•	•	•	· ·
•	•	M Pr	at I I	h na ute	4 m	55 Ę	o Sa	2 2	3pr f	-in 20'	8- 24 ai	20	725 nu	6 2	= A	45 [°] ເົ	7		thu 8 `1	200 : 30 Put	y a tu	m. M.	₹ ,	トイン	r u : 3	nk op s	ver m	s jec	E E	line	•	•	•	• •	· · ·	•	•	•	•	•	•	· · ·		•	•	•	•	•	•	•	· · ·
	•	M R	at I I	h na ute	4 m ite	55 Ę	o Sa	, 2	3pr f	-in 20'	8- 24 ai	2	725 mu	5 - e	= A	45° C``	7 5+0		(lu 8 `1	200 : 30 Put	8 a tu		₹ 7, ,	をから	Yu 3	nk op s	er m	s jec	E I	line	• • •	•	•		· · ·		· · · · · · · · · · · · · · · · · · ·	•	•	•	•	· · ·		•	•	•	•	•	•		· · ·
	•	M Pr	at I I	h na ùte	4 m	55 Į	o t	2	3pr F	-in 20'	24	2	72 5 mi	2	= ¹	45 ² 0	7		(lu 8: 1	20 : 30 Put	8 tu		₹ 7,7	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	F 10 3	nk op s	ver m ule	s jec	E (line	•	•	•				· · · · · · · · · · · · · · · · · · ·	· · ·	· · ·	•	•	· · ·		· · ·	•	•	•	•	•	· · · · · · · · · · · · · · · · · · ·	
		M R	ad uti I	h na ùte	4 m	55 Į	D Saa	2	3pe {	-in 20 20	8- 24 ai	2 2 1	725 MU	5 - e	= 4 De	45 [°] ~	7		(lu 8: 11	20 : 30 Put	Ja tu	6 m. 7m.	₽ -,	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	r u 3	op s	er m	s jec		line	•	•	•						•		•	· · · · · · · · · · · · · · · · · · ·		•		•	•	•	•	-	
		R	at I	h na ùte	4 m ble	55 E	D Saa	?	3pr f	-20 20	8- 24 ai	2	72 5 mJ	e		45° ~	7 5+6		(lu 8: 11	200 - 30 Put	3 Dan true		₽ -,	N 4 5	r u. 3	ops	ver	s jec		line	•							• • • • • • • •		•	• • • • • • • • •			•	• • • • • • •						
		M R	lati I	h na ùte	4 m 172	55 E	⊃ ⇒a	2	3pr {	-in 20'	8-24	2	72 5 MU	2	= A	45° ~	7		(fu 8: 11	200 : 34 Put	7 Da tu	с Эти 2	₹ ,		3	uk op s	er m	s jec ^t	· · ·	line												· · · · · · · · · · · · · · · · · · ·									
		R	adi nti I	h na ùte	4 m he	55 Este			3pr f	- 20 	8- 24 ai	2 2 1	m	2	= A	45° ~	- 7 5+6			ler 2 30 Put	Ja.	с Эти З	₽ ,		ru 3	uk ops	ver m	s je⊂		line	•											· · · · · · · · · · · · · · · · · · ·									
		MR	adt uti I	h na ùte	4 m He	55 E		2	3pr {	20	8-24		nu	2		45° ~	7			20 - 30 Put	3 tu				Fu 3	ops	er m	s jec		line	· · · · · · · · · · · · · · · · · · ·										• • • • • • • • • •									· · · · ·	
		R	at I	h na ite	4 m 72	55 E		2	3pr {	20	8- 24 ai		nu	C -		4 5ື ເ	7		(fu 8: 1	20 - 32 Put	Jan true		₽ ,			ops	ver	s jec		line	•																				
		R	att I	h na ùte	4 m h2	55 E			3pr {	-in 20 	8-24	2	nul	e e	= A	45 [°] ູີ	7		(fu 8: 1	20 - 30 Put	Jan true	2	★ - ,		Yu 3	ops	er nie	s jec		line																					
		R	ad uti I	la na inte	4.	55 E			Zpr {	-in 20'	24		nine Nine Nine Nine Nine Nine Nine Nine	e		45 [°] ~	7			20 - 30 Put		3	♣ -,			ops	er ne	\$ je⊄		line	· · · · · · · · · · · · · · · · · · ·																				

More examples of fields: F((x)) > F(x) > F where F is a field.
Laurant series in x rational functions in x (a symbol)
Eg. $f(x) = \frac{x}{1-x-x^2} \in Q(x)$ can be regarded as an infinite series in x with coefficients in Q
$= F_{0} + F_{1}x + F_{2}x^{2} + F_{3}x^{3} + \cdots \text{where} F_{i} \in \mathbb{O}$ $f'(x) = \frac{(1-x-x^{2})^{1} - x(-1-2x)}{(1-x-x^{2})^{2}} = \frac{1+x^{2}}{(1-x-x^{2})^{2}}$
$f''(x) = \frac{(1-x-x^2)^2(2x) - (1+x^2)2(1-x-x^2)(-1-2x)}{(1-x-x^2)^4} = \frac{(1-x-x^2)(2x) + 2(1+x^2)(1+2x)}{(1-x-x^2)^3} = \frac{2x-2x^2-2x^3+2(1+2x+x^2+2x^3)}{(1-x-x^2)^3}$
$(1-x-x^2)^4$ $(1-x-x^2)^3$
$= \frac{2+6x + 2x^{3}}{(1-x-x^{2})^{3}}$
f''(x) = etc.
$f''(x) = etc.$ $f''(x) = etc.$ $f'(x) = etc.$ $Taylor series centered at 0 for f(x) = \sum_{n=0}^{\infty} \frac{f''(0)}{n!} x^n = f(0) + f'(0)x + \frac{f''(0)}{2}x^2 + \frac{f''(0)}{6}x^3 + \frac{f''(0)}{24}x^4 + \cdots$
$A^{20} = 0 + 1 x + \frac{2}{2} x^{2} + \frac{12}{7} x^{4} + \frac{3}{7} $
The Fibonacci sequence F_{1} is defined recursively $= 7 + 1x + \frac{2}{2}x^{2} + \frac{12}{5}x^{3} + \frac{72}{5}x^{4} + \frac{72}{5}x^{4} + \frac{72}{5}x^{4} + \frac{72}{5}x^{5} + \frac{72}{5}x^{5} + \frac{72}{5}x^{7} + \frac{72}{5}x^{7$
$f_{m} = \begin{cases} 0 \\ f_{n-1} \\ f_{n-2} \\ f_{n-1} \\ f_{n-2} \\ f_{n-1} \\ f_{n-2} \\ f_{n-2} \\ f_{n-1} \\ f_{n-2} \\ $

Alternatively: $f(x) = \frac{x}{1-x-x^2} = q_0 + q_1 x + q_2 x^2 + q_3 x^3 + q_4 x^4 + \cdots = x + x^2$	$+ 2x^3 + 3x^4 + 5x^5 + 8$	X 4
Alternatively $S(x) = \frac{x}{1 - x - x^2} = q_0 + q_1 x + q_2 x^2 + q_3 x^3 + q_4 x^4 + \dots = x + x^2$ $x = (1 - x - x^2)(q_0 + q_1 x + q_2 x^2 + q_3 x^3 + q_4 x^4 + \dots)$ $q_{0=0}$ $T_{q=1}$ $T_{q=1}$		
$= \frac{q_{0} + (q_{1} - q_{0})x + (q_{2} - q_{1} - q_{1})x^{2} + (q_{3} - q_{2} - q_{1})x^{3} + (q_{4} - q_{3} - q_{2})x^{4} + \cdots}{""}$		• •
		• •
Third way: $\frac{1}{1-u} = 1 + u + u^2 + u^3 + u^4 + \dots$ (geometric series)		• •
Since $(1-u)(1+u+u^2+u^3+u^4+) = -u+u^2+u^2-u^3+u^3+$	≓]	• •
Cubstituto u= x+r2		
$\frac{x}{x} = x \left(1 + (x + x^2) + (x + x^2)^2 + (x + x^2)^2$		• •
$= \chi \left(1 + (x + x') + (x + 2x + x') + (x' + 3x' + 5x' + x') + (x' + 4x' + 0x' + (x' + x') + (x' + x'$	•••••••••••••••••••••••••••••••••••••••	• •
$= x(1 + x + 2x^{2} + 3x^{3} + 5x^{4} + \cdots)$		• •
$= \pi + x^{2} + 2x^{3} + 3x^{4} + 5x^{5} + \cdots$	== A (1-E) => 1= A(4-	· ·
= x + x + 2x + 2x + 3x + 3x + 3x + 3x + 3	$=7 A = \frac{1}{a^2 f}$	苏
$\overline{1-x-x^2} = (\overline{1-\alpha x})(\overline{1-\beta x}) = \overline{1-\alpha x} = 1-\beta x \qquad (for x = \frac{1}{\beta})$	$\overline{\beta} = D(\overline{\beta}) \Rightarrow I_{c} B(\beta) = BC$	-α) . []
n, p are me recipione roos of a n n (n-n-1)		-
$\chi = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}, \alpha - \beta = \sqrt{5}$	<i>в</i> о	
$\frac{x}{1-x-x^{2}} = \frac{x}{(1-\alpha x)(1-\beta x)} = \frac{1}{\sqrt{5}} \left(\frac{1}{1-\alpha x} - \frac{1}{1-\beta x}\right) = \frac{1}{\sqrt{5}} \left(\frac{z}{1-\alpha x} \alpha^{n} x^{n} - \frac{z}{1-\beta x} \beta^{n} x^{n}\right) = \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} (\alpha^{n} - \beta^{n}) x^{n} = \frac{1}{\sqrt{5}} \sum_$	$\sum_{n=0}^{\infty} f_n x^n = x + x^2 + 2x^3 + 3x^4 + 3x^$	Sx+.
$F = \alpha^{-}\beta^{+}$	1β)<1 5 β~>c	2
$\overline{F_n} \rightarrow \alpha \qquad \overline{F_n} \sim \frac{1}{\sqrt{5}} \alpha^n \qquad \overline{F_n} = \frac{\alpha^n}{\sqrt{5}} \qquad \text{nearest integer.} \qquad \text{where } \overline{F_n} = \frac{\alpha^{-\beta}}{\sqrt{5}}$	K/>1 So a"- no grows	

Eg.	Count the much	ber ^{an} of sequence	s of 0's and 1's	of length n	having no tu	ro consecutive 1's.
n C	20 20	€				
	000, 100, 010, 00					
	• · · ·					
Other	series are	relevant in combi	natorial applicat	ins in which	Ffx) cannot	converge anywhere og.
)- Ž	n! x" = 1+ 0	$x + 2x^2 + 6x^3 + 24$	x ⁴ +			converge anywhere og.
					0	
f(x) =	$(1 + x + 2x^2 + 6)$	$(5x^3+)^2 = 1 + 2x + 5x^2 +$	•••••••••••••••••••••••••••••••••••••••	· · · · · · · · · ·		
$\frac{1}{2}$	+ 1+ 2x+ 6x	+ 24x ³ +				
					· · · · · · · · ·	· · · · · · · · · · · · · · ·
· · · · ·	$-x-x^2 = x$	$+ x^2 + 2x^3 + 3x^4 +$	5x + 8x +			
1	$\frac{1}{x^2} = 1 + x + 2x^2$	+ 3x ³ +				
. X X ²	$-x^{2} = \frac{1}{\pi} + 1 + 2x$					