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 $|G| \le n$.)

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 $n = ab$, $a, b \ge 1$ 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, $\text{char}\, F$ = 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 ($\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \cdots, p-1\}$ = "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 $\text{char}\, F = 0$ then $F \supseteq \mathbb{Q}$. Eg. $\mathbb{R}, \mathbb{C}, \mathbb{Q}$, number fields, $\mathbb{A} = \{$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 <u>degree</u> $[E:F]$ 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 <u>unique</u> field of order $q = p^k$ (up to isomorphism)

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

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

$+$	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 $1, \alpha$

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

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

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, $x+1$ (both irreducible)

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

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

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 $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$
<u>except</u> 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.

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

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

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

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

$\theta^0 = 1$

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

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

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

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

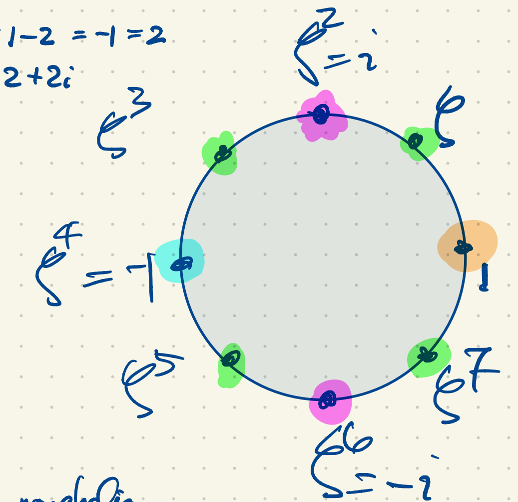
$\theta^5 = \theta^4 \cdot \theta = -\theta = 2\theta = 2+2i$

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

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

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

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

$$\mathbb{F}_4 = \mathbb{F}_2[\alpha] = \{0, 1, \alpha, \beta\} \quad \text{the map} \quad \begin{aligned} 0 &\mapsto 0 \\ 1 &\mapsto 1 \\ \alpha &\mapsto \beta \\ \beta &\mapsto \alpha \end{aligned} \quad . - - - - . .$$

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

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 $G = \{\iota, \sigma, \sigma^2, \dots, \sigma^{k-1}\}$, $\sigma^k = \iota$. Here $\sigma(x) = x^p$.

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

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

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

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

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

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

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

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

$\sigma : \mathbb{F}_q \to \mathbb{F}_q$ is a homomorphism.

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

$x^p = 0$

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 $\mathbb{F}_q$.

$\operatorname{Aut} \mathbb{F}_q \geq \{\iota, \sigma, \sigma^2, \sigma^3, \dots\}$ 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 of order $q-1$ (actually cyclic)

$x^{q-1} = 1$ 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 $\beta = \alpha^2 = \alpha + 1$

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

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

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

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

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

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

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

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

$\sigma(x) = x^3$

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

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

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

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

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

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

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

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

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

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