Field Theory

Book 3

If $\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$ for some $n \geq 1$, then the smallest such n is called the characteristic of the field F, denoted $\operatorname{char} F = n$.

eg. $\operatorname{char} \mathbb{F}_9 = 3$. In $\mathbb{F}_9$, we have 0,

$1+1=2$

$1+1+1=3=0$

$1+1+1+1=4=1$

$\vdots$

$\operatorname{char} \mathbb{F}_p = p$.

If there is no positive n for which $\underbrace{1+1+\cdots+1}_{n} = 0$ then F has characteristic zero ($\operatorname{char} F = 0$).

If $\operatorname{char} F = n > 0$ (F has positive characteristic) then $\operatorname{char} F = p$ is prime. Why?

If $\operatorname{char} F = 6$ then $\underbrace{1+1+1+1+1+1}_{6} = 0$ in F then $(1+1)(1+1+1) = 1+1+1+1+1+1 = 0$

$\Rightarrow 1+1=0$ or $1+1+1=0$.

Given any field F, one of two things can happen:

(i) $\operatorname{char} F = p$ is prime. In this case the smallest subfield of F has p distinct elements 0,

1

$1+1=2$

$1+1+1=3$

$\vdots$

$\underbrace{1+1+\cdots+1}_{p-1} = p-1$

This gives the smallest subfield in F:

$\mathbb{F}_p = \{0, 1, 2, \cdots, p-1\} \subseteq F$.

(ii) $\operatorname{char} F = 0$. $\Rightarrow \mathbb{Q} \subseteq F$ is the smallest subfield.

In every case the unique smallest subfield is known as the prime subfield of F (either $\mathbb{F}_p$ or $\mathbb{Q}$) and F is an extension of its prime subfield.

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

a	a^2	a^3	a^4
0	0	0	0
1	1	1	1
α	β	1	α
β	α	1	β

$+$	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

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

$\mathbb{F}_4$ has characteristic 2.

$\mathbb{F}_2$ is a subfield (the smallest subfield of $\mathbb{F}_4$, called the prime subfield).

So $\mathbb{F}_4$ is a vector space over $\mathbb{F}_2$.

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

$\mathbb{F}_4 = \{c1 + b\alpha : a, b \in \mathbb{F}_2\}$

$= \{0, 1, \alpha, \underbrace{1+\alpha}_{\beta}\}$

Let F be any finite field i.e. $|F| < \infty$.

Then $\operatorname{char} F \neq 0$. In a field of characteristic 0, the elements $0, 1, 1+1, 1+1+1, 1+1+1+1, \ldots$ are all distinct.

So $\operatorname{char} F = \mathbb{F}_p = \{0, 1, \cdots, p-1\}$, p prime. $\mathbb{F}_p$ is the prime subfield of F.

$[F : \mathbb{F}_p] = n \geq 1$, $F = \{a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n : a_1, \ldots, a_n \in \mathbb{F}_p\}$

$\alpha_1, \ldots, \alpha_n$ basis for F over $\mathbb{F}_p$.

$\Rightarrow |F| = p^n$

Every finite field F has prime-power order $|F| = p^n$, p prime, $n \geq 1$.

When $n = [F : \mathbb{F}_p] = 1$, $F = \mathbb{F}_p = \{0, 1, \cdots, p-1\}$ = "integers mod p".

The orders of the finite fields are $2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, \ldots$

(No fields of order $6, 10, 12, 14, 15, 18, \ldots$)

For every $q = p^n$ (p prime, $n \geq 1$) there is a field of order q and it is unique (prime power) and it is unique up to isomorphism. (Proof omitted as this would take too long. We did the case $q = 2^2 = 4$.)

This field is denoted $\mathbb{F}_q$.

Basic facts about $\mathbb{F}_q$: $(q = p^n)$

$\operatorname{char} \mathbb{F}_q = p$.

- For every $a \in \mathbb{F}_q$, $a^q = a$. This generalizes Fermat's Little Theorem (the special case $n=1$ i.e. $q = p$). The same proof.

You are by now familiar with $\mathbb{F}_p$ $(n=1)$.

What about $\mathbb{F}_{p^2} = \{a \cdot 1 + b\theta : a, b \in \mathbb{F}_p\}$?

θ is chosen as a root of an irreducible poly. $f(x) = x^2 + ax + b \in \mathbb{F}_p[x]$.

Special case: Find an irreducible poly. $x^2 + ax + b \in \mathbb{F}_2[x]$

There are only four polynomials of degree 2 in $\mathbb{F}_2[x]$:

$$\left.\begin{aligned} x^2 &= x \cdot x \\ x^2 + 1 &= (x+1)(x+1) \\ x^2 + x &= x(x+1) \end{aligned}\right\} \text{reducible}$$

$x^2 + x + 1$ must be irreducible. The only degree 1 polynomials are x, $x+1$

$f(x) = x^2 + x + 1$ has no roots in $\mathbb{F}_2$ so $f(x)$ is irreducible in $\mathbb{F}_2[x]$.

$f(0) = 1$
$f(1) = 1$

Let α be a root of $f(x)$ not in $\mathbb{F}_2$ but in some extension field. $f(\alpha) = \alpha^2 + \alpha + 1 = 0$

$\mathbb{F}_4 = \{a \cdot 1 + b \cdot \alpha : a, b \in \mathbb{F}_2\}$

Over $\mathbb{F}_2 = \{0,1\}$,

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

degree 2 : $x^2, x^2+1, x^2+x, x^2+x+1$ (only x^2+x+1 is irreducible)

degree 3 : x^3, $x^3+1 = (x+1)(x^2+x+1)$, $x^3+x = x(x+1)^2$, x^3+x+1, $x^3+x^2 = x^2(x+1)$, x^3+x^2+1, $x^3+x^2+x = x(x^2+x+1)$, $x^3+x^2+x+1 = (x+1)^3$

(only two these are irreducible: x^3+x+1, x^3+x^2+1).

degree 4: Sixteen polynomials of degree 4 $x^4+ax^3+bx^2+cx+d$ $(a,b,c,d \in \mathbb{F}_2)$

$x^4+x^2+1 = (x^2+x+1)^2$ has no roots in $\mathbb{F}_2$ but it is reducible.

x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$ are the only irreducible polynomials of degree 4 in $\mathbb{F}_2[x]$.

$\mathbb{F}_8 = \{a\cdot 1 + b\theta + c\theta^2 : a,b,c \in \mathbb{F}_2\}$, $\theta^3+\theta+1=0$ (θ is a root of my favorite irreducible poly. of degree 3 over $\mathbb{F}_2$.)

$\mathbb{F}_8 = \{0, 1, \theta, \theta+1, \theta^2, \theta^2+1, \theta^2+\theta, \theta^2+\theta+1\}$

θ^3 θ^3 θ^6 θ^4 θ^5

$\theta^3 = \theta+1$

$\theta^4 = \theta^2+\theta$

$\theta^5 = \theta^3+\theta^2 = (\theta+1)+\theta^2 = \theta^2+\theta+1$

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

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

Fact: The nonzero elements of any finite field form a cyclic group. ($\mathbb{F}$ consists of all the powers of one element called a primitive element (generator).

Eg. $\mathbb{F}_5 = \{0,1,2,3,4\}$

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

	2^0	2^1	2^2	2^3
$\times$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

$\mathbb{F}_8$

$\times$	1	θ	θ^2	θ^3	θ^4	θ^5	θ^6
1	1	θ	θ^2	θ^3	θ^4	θ^5	θ^6
θ	θ	θ^2	θ^3	θ^4	θ^5	θ^6	1
θ^2				etc.			
θ^3							
$\vdots$				$\vdots$			

$\times$	1	α	β	γ
1	1	α	β	γ
α	α	1	γ	β
β	β	γ	1	α
γ	γ	β	α	1

mult. table for a Klein 4-group (noncyclic group of order 4).

This cannot be a subgroup in the multiplicative group of any field F for the following reason:

It has four solutions of $x^2 = 1$ (roots of $x^2 - 1$)

Wedderburn's Theorem: If F is any field (finite or infinite, then any subgroup of $F^\times$ (the multiplicative group of nonzero elements) is cyclic.

[If $F = \mathbb{F}_q$, then $F^\times$ is cyclic of order $q-1$.

[The n^{th} roots of unity in $\mathbb{C}$ form a cyclic group of order n.

An extension $F \supseteq \mathbb{Q}$ (i.e. a field of characteristic zero) can be a finite extension or an infinite extension i.e.

- $n = [F:\mathbb{Q}] < \infty$: F is a finite extension of $\mathbb{Q}$ (i.e. an extension of finite degree n). These are number fields, also called algebraic number fields.

In this case F is a "simple" extension $F = \mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}\}$.

eg. $F = \mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a,b,c,d \in \mathbb{Q}\}$

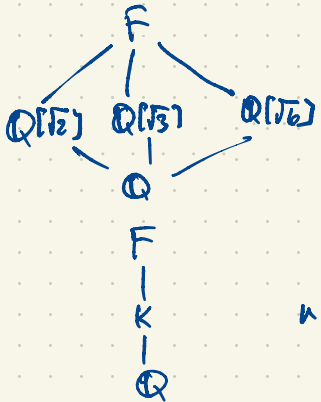
so $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for F over $\mathbb{Q}$ and $[F:\mathbb{Q}] = 4$ (a quartic extension of $\mathbb{Q}$)

quadratic : degree 2
cubic : " 3
quartic : " 4
quintic : " 5

"Almost" any element $\alpha \in F$ generates F as a field: $F = \mathbb{Q}[\alpha]$.

If $\alpha = \sqrt{2} + \sqrt{3}$ then α has min. poly. $x^4 - 10x^2 + 1$

$\alpha = \sqrt{2} + \sqrt{3}$
$\alpha^2 = 2 + 3 + 2\sqrt{6}$
$= 5 + 2\sqrt{6}$
$\alpha^2 - 5 = 2\sqrt{6}$
$\alpha^4 - 10\alpha^2 + 25 = 24$
$\alpha^4 - 10\alpha^2 + 1 = 0$



All five subfields of F.

If $n = [F:\mathbb{Q}] < \infty$ then F has only finitely many subfields and all have degree dividing n

$n = [F:\mathbb{Q}] = [F:K][K:\mathbb{Q}] \Rightarrow [K:\mathbb{Q}]$ divides n.

Every element $\alpha \in F$ (if $n = [F:\mathbb{Q}] < \infty$) is algebraic over $\mathbb{Q}$.

Why? If $\alpha \in F$, $[F:\mathbb{Q}] = n$, then $1, \alpha, \alpha^2, \dots, \alpha^n$ are linearly dependent over $\mathbb{Q}$.

$\Rightarrow$ $a_0 1 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n = 0$ for some $a_0, a_1, \dots, a_n \in \mathbb{Q}$ not all zero.

$\Rightarrow$ α is algebraic.

More than this, α is algebraic of degree dividing n.

$F \supseteq \mathbb{Q}[\alpha] \supseteq \mathbb{Q}$ $\Rightarrow$ $n = [F:\mathbb{Q}] = [F:\mathbb{Q}[\alpha]]\,[\mathbb{Q}[\alpha]:\mathbb{Q}]$

$[\mathbb{Q}[\alpha]:\mathbb{Q}]$ = degree of α over $\mathbb{Q}$ = degree of the min. poly. of α over $\mathbb{Q}$.

- $[F:\mathbb{Q}] = \infty$ eg. $\mathbb{R}, \mathbb{C}, \dots$