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.

$[\mathbb{C}:\mathbb{R}] = 2$ $\quad$ $[\mathbb{R}:\mathbb{Q}] = \infty$ $\quad$ $[\mathbb{C}:\mathbb{Q}] = \underbrace{[\mathbb{C}:\mathbb{R}]}_{2}\underbrace{[\mathbb{R}:\mathbb{Q}]}_{\infty} = \infty$

$\{1, i\}$ basis

$1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{10}, \sqrt{11}, \ldots$ are lin. indep.

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

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

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