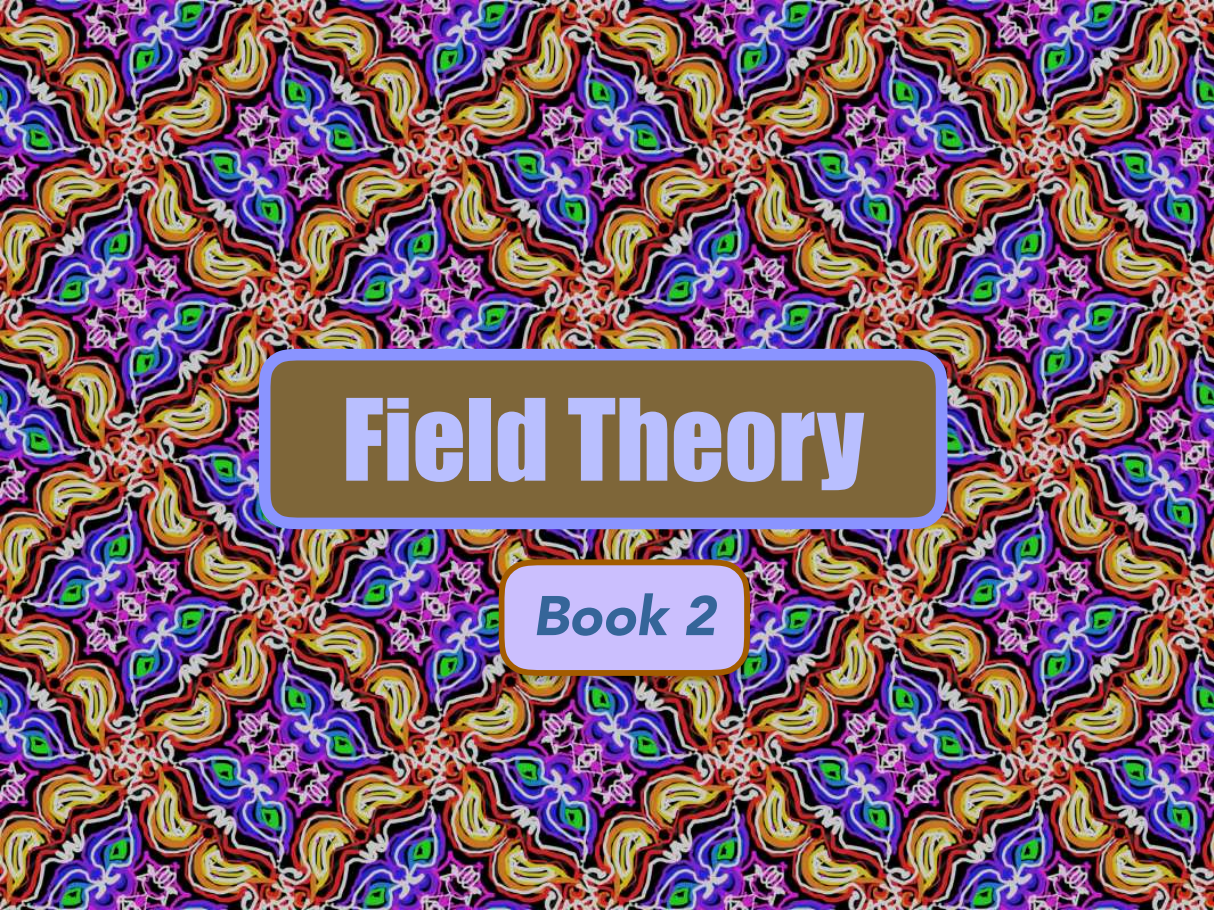




Field Theory

Book 2

Claim: $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$ i.e. $\sqrt{3} = a + b\sqrt{2}$ has no solution with $a, b \in \mathbb{Q}$.

Suppose $\sqrt{3} = a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$. Then $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ so $2ab\sqrt{2} = 3 - a^2 - 2b^2$.

If $ab \neq 0$ then $\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}$, a contradiction.

If $b = 0$ then $0 = 3 - a^2$ so $a^2 = 3$, $a = \pm\sqrt{3} \notin \mathbb{Q}$, a contradiction.

If $a = 0$ then $0 = 3 - 2b^2$ so $2b^2 = 3$, $4b^2 = 6$, $2b = \pm\sqrt{6} \notin \mathbb{Q}$, a contradiction. $\square$

So $1, \sqrt{2}, \sqrt{3} \in \mathbb{R}$ are linearly independent over $\mathbb{Q}$.

- $1 \neq 0$
- $\sqrt{2} \neq \text{scalar multiple of } 1$. ($\sqrt{2} \notin \mathbb{Q}$ by Euclid)
- $\sqrt{3} \neq \text{linear combination of } 1, \sqrt{2}$. (proved above)

$$\sqrt{8} = 2\sqrt{2}$$

$1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17}, \sqrt{19}, \sqrt{23}, \dots$ are linearly independent.

$[\mathbb{R} : \mathbb{Q}] = \infty$ (in fact uncountable)

Also $1, \pi, \pi^2, \pi^3, \dots$ are linearly independent over $\mathbb{Q}$. (since π is transcendental).

An extension $E \supseteq F$ is finite if $[E : F] < \infty$, i.e. $[E : F] = n$ is a positive integer.

eg. $\mathbb{C} \supseteq \mathbb{R}$ is a quadratic extension, hence finite, $[\mathbb{C} : \mathbb{R}] = 2$.

A finite extension of $\mathbb{Q}$ i.e. $E \supseteq \mathbb{Q}$ with $[E : \mathbb{Q}] = n$, a positive integer, is called a number field (or algebraic number field). Here every element $\alpha \in E$ is algebraic over $\mathbb{Q}$. Why?

$1, \alpha, \alpha^2, \dots, \alpha^n$ are $n+1$ vectors in an n -dimensional vector space $E \supseteq \mathbb{Q}$ so this list is linearly dependent i.e. $q_0 + q_1\alpha + q_2\alpha^2 + \dots + q_n\alpha^n = 0$ for some $q_0, q_1, \dots, q_n \in \mathbb{Q}$, not all zero, i.e. α is a root of some nonzero polynomial $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in \mathbb{Q}[x]$.

If $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ then the degree of $f(x)$, denoted $\deg f(x)$, is the largest d such that $a_d \neq 0$.

$$\deg(3x^2 + 5x + 7) = 2$$

$$\deg(0x^2 + 5x + 7) = \deg(5x + 7) = 1$$

$$\deg(7) = \deg(7x^0) = 0$$

$\deg 0$ is sometimes left undefined (not 0) or $\deg 0 = -\infty$.

$$\deg[(3x^2 + 5x + 7)(x^3 - 4x - 11)] = \deg(3x^5 + \dots - 77) = 5$$

$$\deg[f(x)g(x)] = \deg f(x) + \deg g(x)$$

If $g(x) = x^3 - 4x - 11$ then $\deg g(x) = 3$

$$\deg(0g(x)) = \deg 0$$

$$\deg 0 + \deg g(x) = \deg 0 + 3$$

$$\deg 0 = (\deg 0) + 3$$

There is no integer value for $\deg 0$ that satisfies this.
(We don't choose $+\infty$; we choose $-\infty$.)

Let $\alpha \in \mathbb{C}$. If α is the root of some nonzero poly. $f(x) \in \mathbb{Q}[x]$ (i.e. $f(\alpha) = 0$) then α is algebraic of degree n where n is the smallest degree of any such polynomial $f(x)$. In this case, the smallest degree monic polynomial having α as a root is the minimal polynomial of α (over $\mathbb{Q}$).

eg. $\sqrt{14}$ is algebraic of degree 2 with min. poly. $x^2 - 14 \in \mathbb{Q}[x]$.

Look at powers $1, \alpha, \alpha^2, \alpha^3, \dots$

$$\alpha = \sqrt{14} \Rightarrow 1, \alpha \text{ lin. indep.}$$

$$1, \alpha, \alpha^2 \text{ lin. dep.}$$

$$\alpha^2 = 0 \cdot \alpha + 14 \cdot 1$$

$\alpha = \sqrt{2} + \sqrt{3}$ is algebraic of degree 4 with min. poly. $x^4 - 10x^2 + 1$. Why is $\alpha = \sqrt{2} + \sqrt{3}$ not a root of any smaller degree poly. with rational coefficients?

If $x^4 - 10x^2 + 1 = f(x)g(x)$ where $f(x), g(x) \in \mathbb{Q}[x]$ then one of $f(x), g(x)$ is a ^(non-zero) constant polynomial. Assuming we start with a monic poly. with integer coefficients, it suffices to check that there is no nontrivial factorization over $\mathbb{Z}[x]$.

If $x^4 - 10x^2 + 1 = f(x)g(x)$, $f(x), g(x) \in \mathbb{Z}[x]$, neither $f(x)$ nor $g(x)$ is constant then either

(i) $\deg f(x) = 1$, $\deg g(x) = 3$; or

(ii) $\deg f(x) = \deg g(x) = 2$. (The case $\deg f(x) = 3$, $\deg g(x) = 1$ is essentially case (i)).

In both cases we obtain a contradiction.

In case (i), $x^4 - 10x^2 + 1 = (x+a)(x^3+bx^2+cx+d)$, $ad=1$, $a=d=\pm 1$.

In this case $m(x)$ has ± 1 as a root but $m(1) = -8 = m(-1)$, a contradiction.

In case (ii), $m(x) = x^4 - 10x^2 + 1 = (x^2+ax+b)(x^2-ax+c)$, $a, b, c \in \mathbb{Z}$ (since there is no x^3 term on the left).

Once again, $bc=1$ so $b=c=\pm 1$. Now

$$m(x) = x^4 - 10x^2 + 1 = (x^2 + ax \pm 1)(x^2 - ax \pm 1). \text{ Comparing } x^2 \text{ terms on both sides,}$$

$$-10 = \pm 2 - a^2 \text{ i.e. } a^2 = 10 \pm 2 = 8 \text{ or } 12.$$

This is a final contradiction so $m(x) = x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

Note: $x^4 + x^2 + 1$ is reducible in $\mathbb{Z}[x]$ as well as in $\mathbb{Q}[x]$: it factors nontrivially as

$$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1).$$

This polynomial has no roots in $\mathbb{Z}$ or in $\mathbb{Q}$ or in $\mathbb{R}$.

$x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$ but reducible in $\mathbb{R}[x]$. Every polynomial of degree ≥ 3 in $\mathbb{R}[x]$ is reducible.

$$x^4 - 10x^2 + 1 = x^4 + 2x^2 + 1 - 8x^2 = (x^2 + 1)^2 - (2\sqrt{2}x)^2 = (x^2 + 1 + 2\sqrt{2}x)(x^2 + 1 - 2\sqrt{2}x)$$

The polynomial $x - \sqrt{2}$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$ and in $\mathbb{R}[x]$. It has a root $\sqrt{2} \in \mathbb{R}$.

Theorem: If $f(x) \in \mathbb{Z}[x]$ is monic, then $f(x)$ is reducible in $\mathbb{Q}[x]$ iff $f(x)$ is reducible in $\mathbb{Z}[x]$. Assume this, and use it!

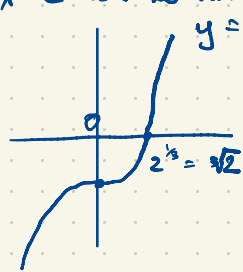
For $f(x) \in \mathbb{Q}[x]$ of degree ≥ 3 , $f(x)$ is reducible in $\mathbb{Q}[x]$ iff it has a root in $\mathbb{Q}$.

This is not true for $\deg f(x) \geq 4$.

Eg. $f(x) = x^4 + x^2 + 1$ has no roots in $\mathbb{Q}$ but it is reducible in $\mathbb{Q}[x]$

eg. $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ since it has no roots in $\mathbb{Q}$. You need to master this point!

$x^3 - 2$ has no rational roots: it has one real root $2^{1/3} \notin \mathbb{Q}$ essentially by Euclid's argument.



$y = x^3 - 2$ If $x = 2^{1/3} \in \mathbb{Q}$, $x^3 = 2$, write $x = \frac{a}{b}$ with a, b positive integers in lowest terms ($\gcd(a, b) = 1$) then $\frac{a^3}{b^3} = 2$ so $a^3 = 2b^3$ is even so a is even.

ie. $a = 2r$ for some positive integer r , so $8r^3 = 2b^3$ and $b^3 = 4r^3$ is even so b is even ie. $b = 2s$ for some $s \in \mathbb{Z}$. This contradicts $\gcd(a, b) = 1$.

Now if $x^3 - 2$ is reducible in $\mathbb{Q}[x]$ then $x^3 - 2 = (x+a)(x^2+bx+c)$, $a, b, c \in \mathbb{Q}$ but then $-a \in \mathbb{Q}$ is a root, contradiction.

For $f(x) \in F[x]$ where F is a field ($f(x)$ is a polynomial in x with coefficients in the field F) and $r \in F$, we have:

r is a root of $f(x)$ iff $x-r$ is a ^{linear factor ie. factor of degree 1.} factor of $f(x)$
 ie. $f(r) = 0$
 ie. r is a "zero" of $f(x)$ ie. $f(x) = (x-r)q(x)$, $q(x) \in F[x]$

In one direction this "iff" statement is obvious: if $f(x) = (x-r)q(x)$ then $f(r) = (r-r)q(r) = 0$.

What about the converse? By the Division Algorithm, $f(x) = q(x)(x-r) + a(x)$, $\deg a(x) < \deg(x-r)$

If r is a root of $f(x)$ then $f(r) = 0 = \underbrace{q(r)}_0 \underbrace{(r-r)}_0 + a \Rightarrow a = 0$
 $\Rightarrow f(x) = q(x)(x-r)$ $\underbrace{0 \text{ or } -00}_0 \underbrace{1}_1$
 $a(x) = a = \text{constant}$

We require the Division Algorithm for this.

Review the Division Algorithm for integers $\mathbb{Z}$:

Let $n, d \in \mathbb{Z}$ with $d \geq 1$. (OK for d negative but we cannot use $d=0$.) In general d won't divide n evenly; there is a remainder.

Theorem There exist unique $q, r \in \mathbb{Z}$ such that $n = qd + r$, $0 \leq r < d$.

Eg. $n=65$, $d=7$, $65 = \underline{9} \cdot 7 + \underline{2}$ $7 \nmid 65$ $\neq$

$$65 = \underline{8} \cdot 7 + \underline{9}$$

$$91 = \underline{13} \cdot 7 + \underline{0}$$

$\begin{matrix} \text{quotient} & \text{remainder} \end{matrix}$ $7 \mid 91$

d divides n ($d \mid n$) $\iff n$ is a multiple of d , $n = qd$ (i.e. $r=0$).

Similarly in $F[x]$, F any field. eg. $\mathbb{Q}[x]$, $\mathbb{R}[x]$, ... not $\mathbb{Z}[x]$.

Theorem (Division Algorithm for polynomials) Let F be any field and let $f(x), d(x) \in F[x]$ where $\deg d(x) \geq 1$. Then there exist unique $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)d(x) + r(x), \quad \deg r(x) < \deg d(x).$$

Eg. $F = \mathbb{Q}$, $f(x) = x^3 - 2x - 3$, $d(x) = x^2 + x + 1$.

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

$$\begin{array}{r} x-1 \\ x^2+x+1 \overline{) x^3-2x-3} \\ \underline{x^3+x^2+x} \\ -x^2-3x-3 \\ \underline{-x^2-x-1} \\ -2x-2 \end{array}$$

$$x^2 + x + 1 = \left(-\frac{1}{2}x\right)(-2x-2) + (1)$$

The Division Algorithm leads to Euclid's Algorithm (for $\mathbb{Z}$, $F[x], \dots$)
not $\mathbb{Z}[x]$

$$\begin{array}{r} -\frac{1}{2}x \\ -2x-2 \overline{) x^2 + x + 1} \\ \underline{x^2 + x} \\ 1 \end{array}$$

$$\gcd(100, 27) = 1 = a \cdot 100 + b \cdot 27 \quad \text{for some } a, b \in \mathbb{Z}$$

$$100 = 3 \times 27 + 19$$

$$27 = 1 \times 19 + 8$$

$$19 = 2 \times 8 + 3$$

$$8 = 2 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

last nonzero remainder

$$\gcd(100, 27) = 1 = 3 - 2$$

$$= 3 - (8 - 2 \times 3)$$

$$= 3 \times 3 - 8$$

$$= 3 \times (19 - 2 \times 8) - 8$$

$$= 3 \times 19 - 7 \times 8$$

$$= 3 \times 19 - 7 \times (27 - 19)$$

$$= 10 \times 19 - 7 \times 27$$

$$= 10 \times (100 - 3 \times 27) - 37 \times 27$$

$$= 10 \times 100 - 37 \times 27$$

$$= 1$$

Continue
Monday

Shorthand

100	27	
1	0	100
0	1	27
1	-3	19
-1	4	8
3	-11	3
-7	26	2
10	-37	1
*	*	0

$$\gcd(100, 27) = 1 = 10 \times 100 - 37 \times 27$$

Euclid's Algorithm uses repeated application of the Division Algorithm. The last nonzero remainder is the gcd.

The gcd of two polynomials is the largest monic polynomial dividing both of them.
 Given $f(x), g(x) \in F[x]$ (F any field), $f(x), g(x)$ not both zero.

$d(x) = \gcd(f(x), g(x))$ is the largest monic polynomial such that $d(x) \mid f(x)$, $d(x) \mid g(x)$.
 We compute $d(x)$ using Euclid's Algorithm and it finds $a(x), b(x) \in F[x]$ such that
 $d(x) = a(x)f(x) + b(x)g(x)$.

Eg. $f(x) = x^3 - 2x - 3$
 $g(x) = x^2 + x + 1$

$$\gcd(f(x), g(x)) = 1 = \left(\frac{1}{2}x\right)f(x) + \left(-\frac{1}{2}x^2 + \frac{1}{2}x + 1\right)g(x) \quad (*)$$

$$f(x) = (x-1)g(x) + (-2x-2)$$

$$g(x) = \left(-\frac{1}{2}x\right)(-2x-2) + (1)$$

$$-2x-2 = (-2x-2)(1) + 0$$

$$1 = g(x) + \left(\frac{1}{2}x\right)(-2x-2)$$

$$= g(x) + \left(\frac{1}{2}x\right)(f(x) - (x-1)g(x))$$

$$= \left(\frac{1}{2}x\right)f(x) + \left(1 - \frac{1}{2}x^2 + \frac{1}{2}x\right)g(x)$$

Check: $\left(\frac{1}{2}x\right)(x^3 - 2x - 3) + \left(-\frac{1}{2}x^2 + \frac{1}{2}x + 1\right)(x^2 + x + 1) = 1$

x^2 terms: $-1 + 1 + \frac{1}{2} - \frac{1}{2} = 0$

x terms: $-\frac{3}{2} + \frac{1}{2} + 1 = 0$

constant: 1

Alternatively

	$f(x) = x^3 - 2x - 3$	$g(x) = x^2 + x + 1$	
①	1	0	$x^3 - 2x - 3$
②	0	1	$x^2 + x + 1$
③ = ① - (x)②	1	$-x + 1$	$-2x - 2$
④ = ② + $\frac{1}{2}$ ③	$\frac{1}{2}x$	$-\frac{1}{2}x^2 + \frac{1}{2}x + 1$	1
	*	*	0

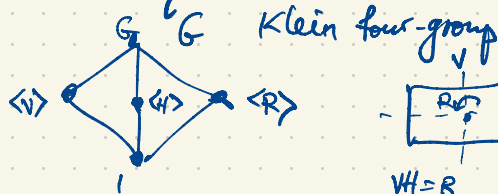
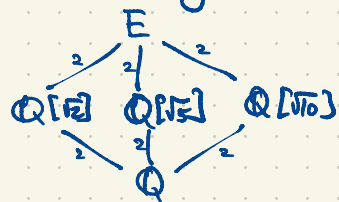
Recall: we considered the field $\mathbb{Q}[\theta] = \{a + b\theta + c\theta^2 : a, b, c \in \mathbb{Q}\}$, θ root of $f(x)$
 We computed $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ where $\alpha = \theta^2 - 3$, $\beta = \theta^2 + \theta + 1 = g(\theta)$
 To find $\frac{1}{\beta}$, use (*)
 $\frac{1}{\beta} = -\frac{1}{2}\theta^2 + \frac{1}{2}\theta + 1$
 $1 = \left(\frac{1}{2}x\right)f(x) + \left(-\frac{1}{2}x^2 + \frac{1}{2}x + 1\right)g(x)$
 $1 = \left(\frac{1}{2}\theta\right)f(\theta) + \left(-\frac{1}{2}\theta^2 + \frac{1}{2}\theta + 1\right)g(\theta)$

$$E = \mathbb{Q}[\sqrt{2}, \sqrt{5}] = \{a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10} : a, b, c, d \in \mathbb{Q}\}$$

$$[E : \mathbb{Q}] = 4 \text{ with basis } \{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$$

E has subfields $\mathbb{Q}$, E , $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{10}]$

These are the only subfields (which is not quite obvious)



$$\begin{array}{c} \text{Klein four-group} \\ \downarrow \\ \boxed{\begin{array}{c} \mathbb{Q}[\sqrt{2}] \\ \mathbb{Q}[\sqrt{5}] \end{array}} \xrightarrow{H} \\ \downarrow \\ \mathbb{Q} \\ \text{WH} = \mathbb{R} \end{array}$$

$$\mathbb{Q}[x], \mathbb{Q}[x, y]$$

$$\mathbb{Q}[x] \rightarrow \mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$$

$$\begin{array}{c} \cup \\ f(x) \mapsto f(\sqrt{2}) \end{array}$$

Evaluation maps are homomorphisms

$$f(x) + g(x) \mapsto f(\sqrt{2}) + g(\sqrt{2})$$

$$f(x)g(x) \mapsto f(\sqrt{2})g(\sqrt{2})$$

$$\mathbb{Q}[x, y] \rightarrow \mathbb{Q}[\sqrt{2}, \sqrt{5}] \subset \mathbb{R}$$

$$f(x, y) \mapsto f(\sqrt{2}, \sqrt{5})$$

homomorphism

$$[E : \mathbb{Q}[\sqrt{2}]] = 2 \text{ with basis } \{1, \sqrt{5}\}$$

Every $\alpha \in E$ i.e. $\alpha = a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}$ can be uniquely written as

$$\alpha = \underbrace{(a + b\sqrt{2})}_\mathbb{Q} + \underbrace{(c + d\sqrt{2})}_\mathbb{Q} \sqrt{5}$$

$$[E : E] = 1 \text{ with basis } \{1\}$$

Every $\alpha \in E$ can be uniquely expressed as

$$\alpha = (\alpha)1$$

$$\text{Note: } [E : \mathbb{Q}] = [E : \mathbb{Q}[\sqrt{2}]] [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]$$

Given a "tower" of fields $E \supseteq K \supseteq F$ we have

$$[E : F] = [E : K][K : F]$$

$$\text{eg. } \underbrace{[\mathbb{C} : \mathbb{Q}]}_\infty = \underbrace{[\mathbb{C} : \mathbb{R}]}_2 \underbrace{[\mathbb{R} : \mathbb{Q}]}_\infty$$

Given a "tower" of fields $E \supseteq K \supseteq F$ we have
 $[E:F] = [E:K][K:F]$.

eg. $\underbrace{[C:\mathbb{Q}] = 6}_{\infty} = \underbrace{[C:\mathbb{R}] = 2}_2 \underbrace{[\mathbb{R}:\mathbb{Q}] = 2}_{\infty}$

If $[K:F] = m$ and $[E:K] = n$ then we have
 a basis $\{\alpha_1, \dots, \alpha_m\}$ we can choose a basis for K over F
 so every $\alpha \in K$ can be uniquely written as
 $\alpha = c_1\alpha_1 + c_2\alpha_2 + \dots + c_m\alpha_m$, $c_1, \dots, c_m \in F$.

Every $\beta \in E$ can be written uniquely as
 $\beta = b_1\beta_1 + b_2\beta_2 + \dots + b_n\beta_n$, $b_j \in K$
 $\{\beta_1, \dots, \beta_n\}$ basis for E over K .

$$b_j = a_{j1}\alpha_1 + a_{j2}\alpha_2 + \dots + a_{jm}\alpha_m, \quad a_{ij} \in F$$

$$= \sum_{i=1}^m a_{ij}\alpha_i$$

$$\beta = \sum_{j=1}^n b_j \beta_j = \sum_{j=1}^n \left(\sum_{i=1}^m a_{ij} \alpha_i \right) \beta_j = \sum_{i=1}^m \sum_{j=1}^n \underbrace{a_{ij}}_F \underbrace{\alpha_i \beta_j}_E$$

Note: $\sqrt[3]{2} \notin \mathbb{Q}[\sqrt{2}, \sqrt{5}]$.

$\mathbb{Q}[\sqrt[3]{2}] \supset \mathbb{Q}$ is an extension of degree 3.

Denoting $\alpha = \sqrt[3]{2} = 2^{1/3}$ we have $\mathbb{Q}[\alpha] = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}$.

$\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$. α has min. poly. $x^3 - 2$.

$E = \mathbb{Q}[\sqrt{2}, \sqrt{5}]$ cannot contain $\alpha = 2^{1/3}$.

If it did, we would have

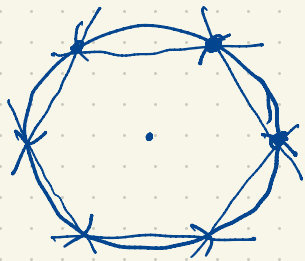
$$E \supseteq \mathbb{Q}[\alpha] \supseteq \mathbb{Q}$$

$$[E:\mathbb{Q}] = [\mathbb{Q}[\alpha]:\mathbb{Q}] [E:\mathbb{Q}[\alpha]]$$

4 ? 3

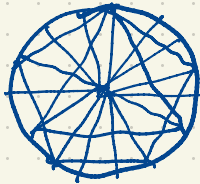
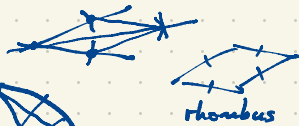
contradiction.

Straightedge and Compass Constructions



Which regular n -gons are constructible using straightedge and compass?

$$n = 3, 8, 10, 4, 17, 5, \dots$$



A regular n -gon is constructible using straightedge and compass iff n is a power of 2 times a product of distinct Fermat primes.

A Fermat prime is a prime number that is one bigger than a power of 2 i.e.

$$2^m + 1$$

$$m = 2^k$$

We will prove that a regular 9-gon is not constructible using straightedge and compass.

k	$F_k = 2^{2^k} + 1$
0	3
1	5
2	17
3	257
4	65537
5	not prime

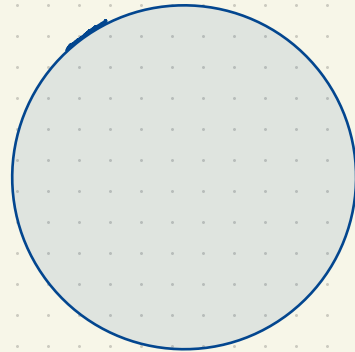
$$(2^2)^k = 2^{2k}$$

$$F_5 = 2^{32} + 1 = 4294967297$$

Are there any other Fermat primes? Unknown.

We suspect not.

This number theory!



Compare: for which n can we construct the roots of a poly. $f(x)$ of degree n using field operations $+, -, \times, \div$ and n^{th} roots

Answer: $n \leq 4$ only. Galois theory shows this, relying on facts about the group S_n which is not solvable for $n \geq 5$.

Compare: $\int x e^{x^2} dx = \frac{1}{2} e^{x^2} + C$.

$\int x^n e^{x^2} dx$ can be written in elementary form iff n is odd.

$\int e^{x^2} dx$ cannot be found in "elementary form"

Field theory

Has been used to prove impossibility of certain tasks eg.

- constructing a regular nonagon (9-gon), trisecting angle, etc. using straightedge and compass;
- "finding" roots of a typical poly. $f(x)$ of degree ≥ 5 using only $+, -, \times, \div, n^{\text{th}}$ roots
- finding $\int e^{x^2} dx$ in "elementary form"

Field theory also provides the tools/techniques/algorithms needed to constructively solve certain problems of these types eg.

- construct regular 17-gon
- finding roots of poly's when expressible using $+, -, \times, \div, n^{\text{th}}$ roots
- expressing antiderivates in elementary form when possible

$$\int e^{x^2} dx = \int_0^x e^{t^2} dt + C$$

a^{b^c} means $a^{(b^c)}$ or $(a^b)^c$

$$(a^b)^c = a^{bc} = (a^c)^b$$

$\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\dots}}}$ is the limit of a sequence $\sqrt{2}, \sqrt{2}^{\sqrt{2}}, \sqrt{2}^{\sqrt{2}^{\sqrt{2}}}, \sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}}}}, \dots$
i.e. the sequence $a_1, a_2, a_3, a_4, \dots$ where $a_1 = \sqrt{2}$

$$a_{n+1} = \sqrt{2}^{a_n}$$

Compare: $x = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\ddots}}}}$ is the limit of the sequence

	1	$1 + \frac{1}{1}$	$1 + \frac{1}{1 + \frac{1}{1}}$	$1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}$	...
	"	"	"	"	
	1	2	$\frac{3}{2}$	$\frac{5}{3}$	

$$1 + \frac{1}{\frac{3}{2}} = 1 + \frac{2}{3} = \frac{5}{3}$$

i.e. $b_0, b_1, b_2, b_3, \dots$ where $b_0 = 1$;

$$b_{n+1} = 1 + \frac{1}{b_n}$$

i.e. $1, 2, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \frac{34}{21}, \frac{55}{34}, \frac{89}{55}, \frac{144}{89}, \dots$

$$K = 1 + \frac{1}{q}$$

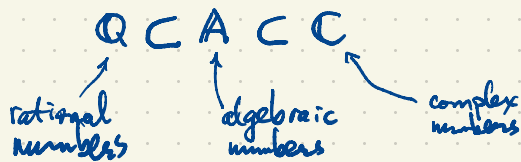
$$\alpha^2 = \alpha + 1$$

$$d^2 - d - 1 = 0$$

α is a root of $x^2 - x - 1$ so $\alpha = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$

Since $\alpha > 0$, $\alpha = \frac{1+\sqrt{5}}{2} \approx 1.618$ (Golden Ratio)

Use similar reasoning in #3, 4.



Can you find irrational numbers a, b such that a^b is rational?

Do these exist irrational $a, b > 0$ (positive real) such that a^b is rational?

... .. $a, b > 0$ such that $a+b$ is rational? $\sqrt{2} + (7-\sqrt{2}) = 7$

... .. a^b is rational? eg $\sqrt{2} \cdot \sqrt{2} = 2$.
 or $\sqrt{2} \cdot \frac{1}{\sqrt{2}} = 1$

Is $\sqrt{2}^{\sqrt{2}}$ rational or irrational?

If $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ then take $a = \sqrt{2}$ and $b = \sqrt{2}$.

If $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ then take $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$, giving $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$.

Theorem There do exist a, b positive real irrational numbers such that a^b is rational.

This is a nonconstructive proof.

Compare: the existence of transcendental numbers has an easy nonconstructive proof.

Liouville's constant $\sum_{n=1}^{\infty} \frac{1}{10^n!} = 0.11000100000000000000000001000\dots$

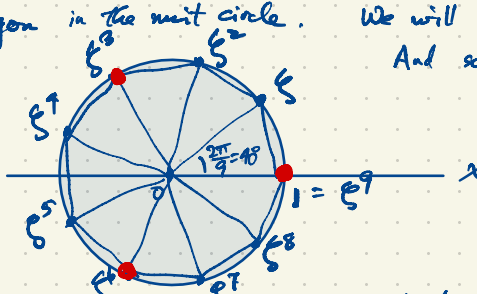
this was the first known explicit transcendental number.

Regular 9-gon in the unit circle

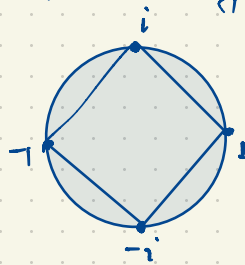
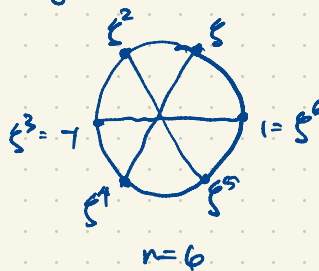
We will show that this figure is not constructible using straightedge and compass.

And so it follows that a 120° angle cannot be trisected using
You cannot trisect 60° angle

Our argument will show that most angles cannot be trisected using straightedge and compass. But some can, eg. 90° angles.



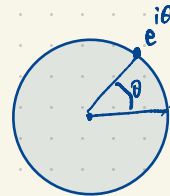
The vertices of the regular n -gon inscribed in a unit circle starting at $(1, 0)$ are the n^{th} roots of unity in $\mathbb{C}$.


$$n = 4$$


De Moivre's formula (see "review" on complex numbers linked on the course website)

$$e^{i\theta} = \cos \theta + i \sin \theta \quad \text{for } \underline{\text{all}} \quad \theta \in \mathbb{C}$$

When $\theta \in \mathbb{R}$, $e^{i\theta} = (\cos \theta, \sin \theta)$ parameterizes the unit circle for $\theta \in [0, 2\pi]$.

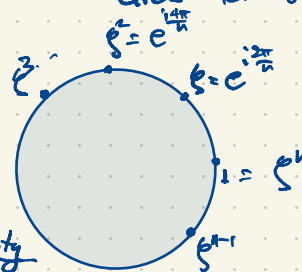


$\xi = e^{\frac{2\pi i}{n}}$ is an algebraic number:
it is a root of $x^n - 1 = (x-1)(x-\xi)(x-\xi^2) \cdots (x-\xi^{n-1})$

$$(\xi^k)^n = (\xi^n)^k = 1^k = 1$$

The n vertices of the regular n -gon are the n^{th} roots of unity in $\mathbb{C}$.

$\{1, \epsilon, \epsilon^2, \dots, \epsilon^{n-1}\}$ is a multiplicative cyclic group $\epsilon^j \epsilon^k = \epsilon^{j+k}$ (exponents mod n).
Any element in this group generates a subgroup. If ϵ^j generates the whole group, it's called a primitive n^{th} root of unity.



$$f^n = (e^{i2\pi})^n = e^{i2\pi} = 1$$

Ex. for $n=9$, the 9th roots of unity form a cyclic group $\langle \zeta \rangle = \{1, \zeta, \zeta^2, \dots, \zeta^8\}$, $\zeta^9 = 1$
 where $\zeta = e^{2\pi i/9}$ $\langle \zeta^3 \rangle = \{1, \zeta^3, \zeta^6\}$

There are six primitive 9th roots of unity: $\zeta, \zeta^2, \zeta^4, \zeta^5, \zeta^7, \zeta^8$. (every 9th root which is not a cube root of 1)

The 9 ninth roots of unity are the roots of

$$x^9 - 1 = (x-1)(x^8 + x^7 + x^6 + \dots + x + 1)$$

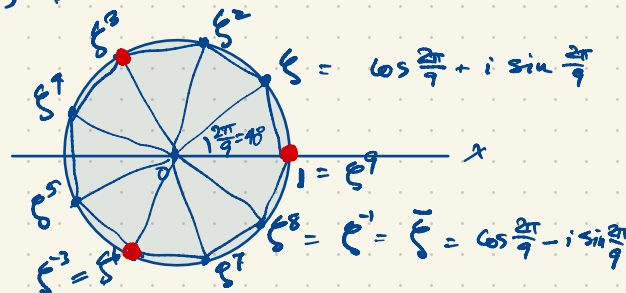
$$= (x^3 - 1)(x^6 + x^3 + 1) = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1) \quad (\text{irreducible factors in } \mathbb{Q}[x])$$

root: 1
 (the 1st root of unity)

roots: ζ^3, ζ^6
 (the primitive cube roots of unity)

roots: $\zeta, \zeta^2, \zeta^4, \zeta^5, \zeta^7, \zeta^8$
 (the primitive 9th roots of unity)

$$\phi(9) = 6$$



$$1 + \zeta^3 + \zeta^6 = 0 \Rightarrow \begin{aligned} \zeta^3 + \zeta^6 &= -1 \\ \zeta^3 + \zeta^{-3} &= -1 \end{aligned}$$

The 9th roots of unity add up to 0:

$$1 + \zeta + \zeta^2 + \dots + \zeta^8 = 0$$

The minimal poly. of ζ (over $\mathbb{Q}$) is $x^6 + x^3 + 1$.

$$\zeta = e^{2\pi i/9} = \cos \frac{2\pi}{9} + i \sin \frac{2\pi}{9} \quad \text{algebraic of degree 6}$$

$$\alpha = 2 \cos \frac{2\pi}{9} = \zeta + \zeta^{-1} = \zeta + \zeta^8 = \zeta + \bar{\zeta}$$

is algebraic of degree 3

$$\alpha = \zeta + \zeta^{-1}$$

$$\alpha^2 = (\zeta + \zeta^{-1})(\zeta + \zeta^{-1}) = \zeta^2 + 2 + \zeta^{-2}$$

$$\alpha^3 = (\zeta + \zeta^{-1})^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3}$$

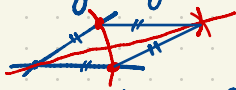
$$\alpha^3 - 3\alpha + 1 = 0 \quad = -1 + 3\alpha$$

the min. poly. of α is $x^3 - 3x + 1$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Now you can do HW2 #5.

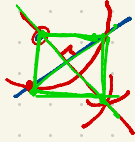
Straightedge & Compass Constructions



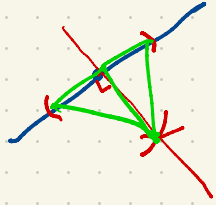
Rhombus

(parallelogram with sides of equal length)

Bisecting an angle

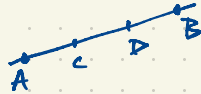
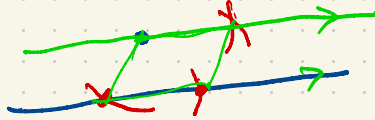


Dropping a perpendicular



Raising a perpendicular

Constructing a parallel line

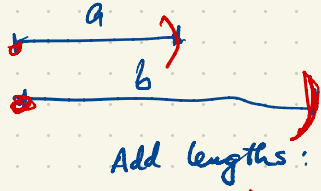


Trisecting a line segment

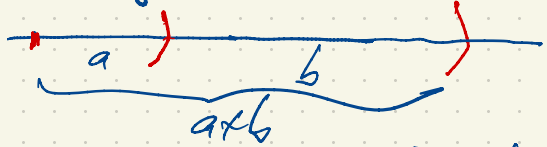
(or divide a line segment into n equal segments for any n)

Given points $A \neq B$, find (construct) points C, D on line AB such that AC, CD, DB all have the same length.

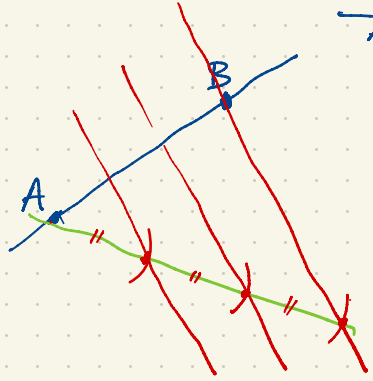
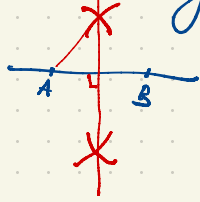
Given a line segment, multiply its length by any rational number.



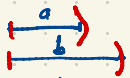
Add lengths:



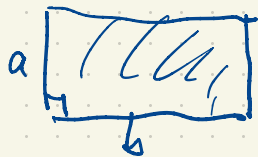
Bisect line segment



Can we multiply the lengths of two line segments?



Given line segments of length a, b , can we construct a line segment of length ab ?

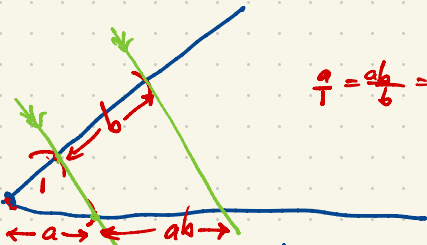


First specify a unit length: 

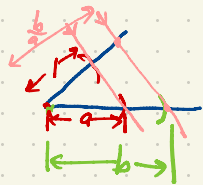
Now:

Draw any angle (not 0° or 180°)

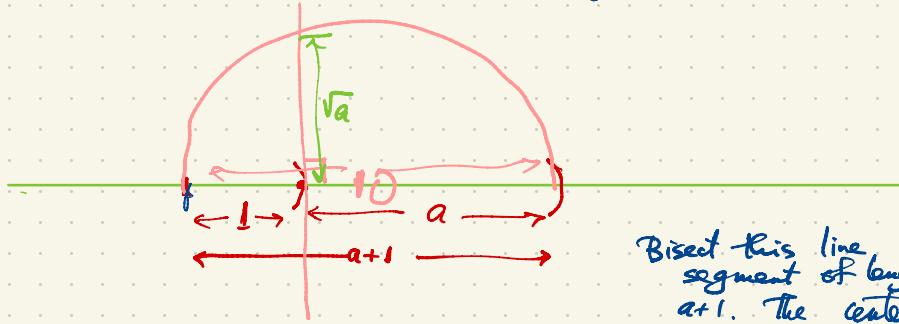
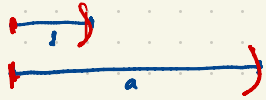
$$\frac{a}{1} = \frac{ab}{b} = \frac{a+ab}{1+b}$$



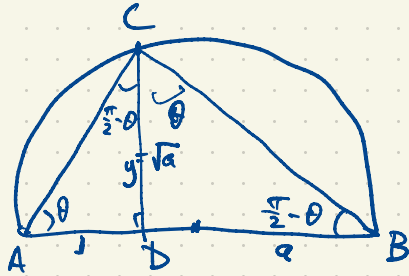
We can also divide $\frac{b}{a}$



Can we find a line segment of length $\sqrt{a}$, given line segments of length 1 and a ?



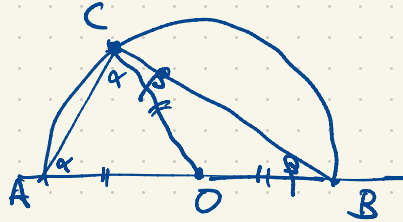
Bisect this line segment of length $a+1$. The center is at a point we'll call O .
Construct the semicircle centered at O of radius equal to the distance shown.



The three triangles in this picture are similar:

$\triangle ADC$, $\triangle CDB$, $\triangle ACB$

$$\frac{1}{y} = \frac{y}{a} \Rightarrow y^2 = a \Rightarrow y = \sqrt{a}$$



$$\alpha + (\alpha + \beta) + \beta = \pi$$

$$\alpha + \beta = \frac{\pi}{2}$$

What can be constructed using straightedge and compass only?

Every step in a construction consists of:

- Given two previous points, we can join them to form the line through them.
- Given two " " " " , we can set the compass radius to their distance.

Then using any previously constructed point as center, we can construct a circle or any arc thereof.

- Given any two previously constructed lines, we can take their intersection point as a new point in the construction. Similarly if we intersect two circles or arcs thereof. Or similarly if we intersect a previously constructed line with a previously constructed circle/arc.

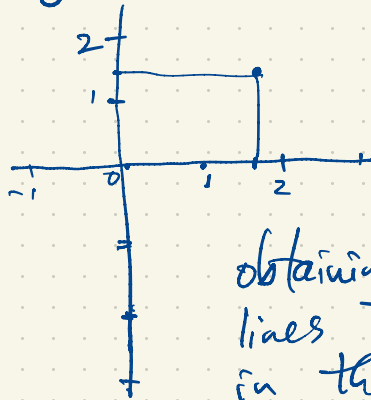
Mon Nov 10: Test 50 min in class.

November 2025

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

www.a-printable-calendar.com

Without loss of generality, we start with a given line segment whose length we call 1.



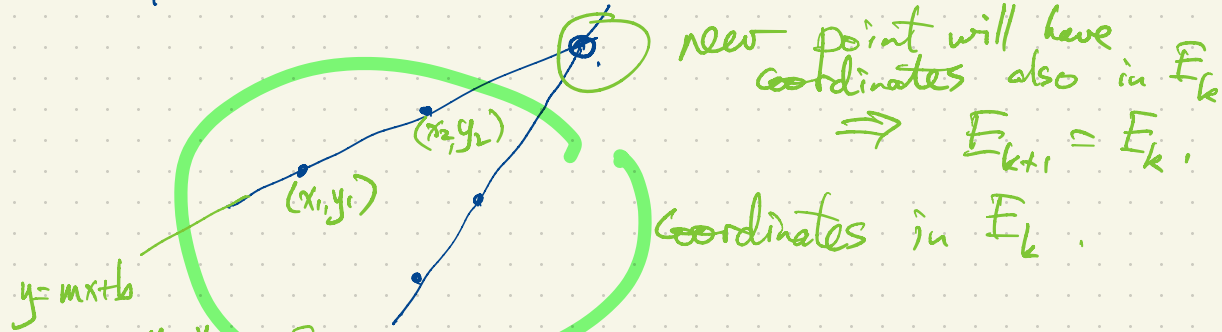
Any point in $\mathbb{Q}^2 = \{(x,y) : x,y \in \mathbb{Q}\}$ is then constructible.

We continue constructing, obtaining new points and lines and circles. All points in this construction will have coordinates in an extension $E \supseteq \mathbb{Q}$ with $[E:\mathbb{Q}] = 2^n$ ($n \geq 0$) as we will prove.

At the start, all points in our construction are in $\mathbb{Q}^2$.
 Let E_k be the field generated by all coordinates of points up to step k .

$$E_0 = \mathbb{Q}.$$

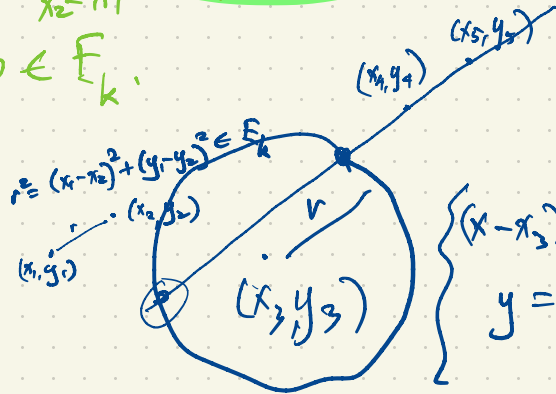
By induction we have $[E_{k+1} : E_k] = 1 \text{ or } 2 \Rightarrow [E_n : \mathbb{Q}] \in \{1, 2, 4, 8, \dots, 2^n\}$.
 We only need to consider a step which produces new points.
 If in step k we are intersecting two lines through previously constructed points



$$m = \frac{y_2 - y_1}{x_2 - x_1} \in E_k$$

$$b \in E_k.$$

If in step k we are intersecting a previous line with a previous circle, the new points (x, y) will have coordinates in E_{k+1} , where $[E_{k+1} : E_k] = 1 \text{ or } 2$.



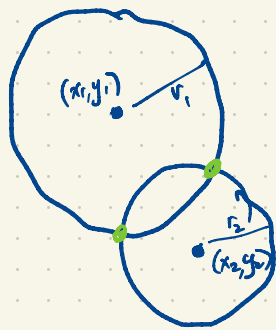
$$\begin{cases} (x - x_3)^2 + (y - y_3)^2 = r^2 & x_3, y_3, r^2 \in E_k \\ y = mx + b \end{cases}$$

$$m = \frac{y_5 - y_4}{x_5 - x_4} \in E_k$$

$$b \in E_k$$

If in step k we are intersecting two previous circles

$$x_1, x_2, y_1, y_2, r_1^2, r_2^2 \in E_k$$



$$\begin{cases} (x-x_1)^2 + (y-y_1)^2 = r_1^2 \\ (x-x_2)^2 + (y-y_2)^2 = r_2^2 \end{cases}$$

$$\Leftrightarrow \begin{cases} x^2 - 2x_1x + x_1^2 + y^2 - 2y_1y + y_1^2 = r_1^2 \\ x^2 - 2x_2x + x_2^2 + y^2 - 2y_2y + y_2^2 = r_2^2 \end{cases}$$

$$\Leftrightarrow \begin{cases} x^2 - 2x_1x + x_1^2 + y^2 - 2y_1y + y_1^2 = r_1^2 \\ 2(x_1 - x_2)x + x_2^2 - x_1^2 + 2(y_1 - y_2)y + y_2^2 - y_1^2 = r_2^2 - r_1^2 \end{cases}$$

$$\boxed{*}x + \boxed{*}y = \boxed{*}$$

x is either in E_k or $E_{k+1} = E_k(\pi) > E_k$, $[E_{k+1} : E_k] = 2$.

To construct a regular pentagon using straightedge and compass,

$$\alpha = 2 \cos \frac{2\pi}{5} = 2 \cos 72^\circ = \frac{-1+\sqrt{5}}{2}$$



$$\frac{1+\sqrt{5}}{2}$$

$$2\alpha = -1 + \sqrt{5}$$

$$\rightarrow \alpha = \frac{-1+\sqrt{5}}{2} = 2 \cos 72^\circ$$

$$\frac{1}{2}\alpha = \cos 72^\circ$$

$$\mathbb{F}_7 = \{a+bi : a, b \in \mathbb{F}_3\} \quad i = \sqrt{-1} = \sqrt{2} \quad -7 = 2$$

$$[\mathbb{F}_7 : \mathbb{F}_3] = 2 \quad \text{with basis } \{1, i\} \quad \dots = -10 = -7 = -4 = -1 = 2 = 5 = 8 = \dots$$

$$\mathbb{F}_7 = \{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\} \quad , 2 = -1$$

$$x^2 + x + 2 \text{ has roots } \frac{-1 \pm \sqrt{1-8}}{2} = \frac{-1 \pm \sqrt{-7}}{2} = \frac{-1 \pm \sqrt{2}}{2} = \frac{-1 \pm i}{2} = \frac{-(-1 \pm i)}{2} = 1+i \text{ or } 1-i$$

$$x^2 + x + 2 = (x - 1 - i)(x - 1 + i)$$

$$\begin{aligned} x^2 + x + 1 &= (x-1)(x-1) \quad \text{roots } \frac{-1 \pm \sqrt{1-4}}{2} = \frac{-1 \pm \sqrt{-3}}{2} = -\frac{1}{2} = 1 \quad (\text{a double root}) \\ &= (x-1)^2 \\ &= x^2 - 2x + 1 \quad \checkmark \end{aligned}$$

Every quadratic $ax^2 + bx + c$, $a, b, c \in \mathbb{F}_3$, $a \neq 0$
has roots in $\mathbb{F}_9$, so it factors into linear factors in $\mathbb{F}_9[x]$
either two distinct roots in $\mathbb{F}_9$ or a double root.

$$\begin{aligned} x^2 + x &= x(x+1) \text{ has roots } 0, 2 \text{ in } \mathbb{F}_3 \subset \mathbb{F}_9. \\ \frac{-1 \pm \sqrt{1}}{2} &= \frac{-1 \pm 1}{2} = 0 \text{ or } -1 = 2 \end{aligned}$$

Test: only on material
up to here

Field Characteristic

Given a field F , what is the smallest subfield $K \subseteq F$?

$$\begin{aligned} 0, 1 \in K &\Rightarrow 1+1=2 \in K \\ 1+1+1 &= 3 \in K \\ 1+1+1+1 &= 4 \in K \\ 1+1+1+1+1 &= 5 \in K \end{aligned}$$

$$\begin{aligned} 1+1+1+1+1+1 &= 6 \in K \\ 1+1+1+1+1+1+1 &= 7 \in K \end{aligned}$$

But these elements might not all be distinct.

If $|F| < \infty$ (a finite field) then
this list contains repetitions.
Where does this list start to repeat?

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

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

$$\begin{aligned} 0 & \\ 1+1 &= 2 \\ 1+1+1 &= 3=0 \\ 1+1+1+1 &= 4=1 \\ &\vdots \end{aligned}$$

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

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

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

If $\text{char } F = 6$ 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) $\text{char } F = p$ is prime. In this case the smallest subfield of F has distinct elements

$$\begin{aligned} 0 & \\ 1 & \\ 1+1 &= 2 \\ 1+1+1 &= 3 \\ &\vdots \\ \underbrace{1+1+\dots+1}_{p-1} &= p-1 \end{aligned}$$

This gives the smallest subfield in F :

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

(ii) $\text{char } F = 0$. $\Rightarrow \mathbb{Q} \subseteq F$ 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 $\mathbb{F}_2$.

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

$$\mathbb{F}_4 = \{a1 + b\alpha : a, b \in \mathbb{F}_2\}$$

$$= \{0, 1, \alpha, 1+\alpha\}$$

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

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

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

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

$\alpha_1, \dots, \alpha_n$ 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 $n = [F : \mathbb{F}_p] = 1$, $F = \mathbb{F}_p = \{0, 1, \dots, p-1\}$ = "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, ...
(No fields of orders 6, 10, 12, 14, 15, 18, ...)

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

- $\text{char } \mathbb{F}_q = p$.
- 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 $\mathbb{F}_4 = \{a1 + b\theta : a, b \in \mathbb{F}_2\}$?

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 $\mathbb{F}_2[x]$:

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

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

$x^2 + x + 1$ 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 $\mathbb{F}_2[x]$.

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 1 \end{aligned}$$

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