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 $\sqrt{2} = \dfrac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$, 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 $\mathbb{Q}$.

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

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

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

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

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

An extension $E \supseteq F$ is <u>finite</u> 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 <u>number field</u> (or <u>algebraic number field</u>). Here every element $\alpha \in E$ is algebraic over $\mathbb{Q}$. Why?

$1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n+1$ vectors in an n-dimensional vector space $E \supseteq \mathbb{Q}$ so this list is linearly dependent i.e. $a_0 1 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$ for some $a_0, a_1, \ldots, a_n \in \mathbb{Q}$, not all zero, i.e. α is a root of some nonzero polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Q}[x]$.

If $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ then the degree of $f(x)$, denoted $\deg f(x)$, is the largest d such that $a_d \neq 0$.

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

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

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

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

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

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

If $g(x) = x^3-4x-11$ then $\underbrace{0g(x)} = 0$

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

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

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

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 $1, \alpha, \alpha^2, \alpha^3, \ldots$ $\quad \alpha = \sqrt{14} \Rightarrow$ $1, \alpha$ lin. indep.

$1, \alpha, \alpha^2$ lin. dep. $\quad \alpha^2 = 0\cdot\alpha + 14\cdot 1$

$\alpha = \sqrt{2}+\sqrt{5}$ is algebraic of degree 4 with min. poly. $x^4 - 10x^2 + 1$. Why is $\alpha = \sqrt{2}+\sqrt{5}$ not a root of any smaller degree poly. with rational coefficients?

If $m(x) = x^4 - 10x^2 + 1 = f(x)g(x)$ where $f(x), g(x) \in \mathbb{Q}[x]$ then one of $f(x), g(x)$ is a (nonzero) 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

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

$-10 = \pm 2 - a^2$ i.e. $a^2 = 10 \pm 2 = 8$ 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 $x - 7$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$ and in $\mathbb{R}[x]$. It has a root $7 \in \mathbb{Z}$.

<u>Theorem</u>: 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 2 or 3, $f(x)$ is reducible in $\mathbb{Q}[x]$ iff it has a root in $\mathbb{Q}$.

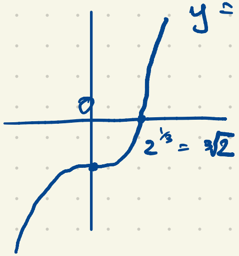
This is not true for $\deg f(x) \geq 4$.

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 $2^{1/3} \notin \mathbb{Q}$ essientially by Euclid's argument.

$y = x^3 - 2$



If $\alpha = 2^{1/3} \in \mathbb{Q}$, $\alpha^3 = 2$, write $\alpha = \frac{a}{b}$ 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. i.e. $a = 2r$ for some positive integer r. So $8r^3 = 2b^3$ and $b^3 = 4r^3$ is even so b is even i.e. $b = 2s$ 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 $\left\{\begin{matrix}\text{factor} \\ \text{divisor}\end{matrix}\right.$ of $f(x)$ (linear factor i.e. factor of degree 1.)

i.e. $f(r) = 0$ i.e. $f(x) = (x - r)q(x)$, $q(x) \in F[x]$

i.e. r is a "zero" of $f(x)$

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

What about the converse? By the Division Algorithm, $f(x) = q(x)(x-r) + a(x)$, $\underbrace{\deg a(x)}_{0 \text{ or } -\infty} < \underbrace{\deg (x-r)}_{1}$

$a(x) = a = \text{constant}$

If r is a root of $f(x)$ then $f(r) = 0 = q(r)\underbrace{\cancel{(r-r)}}_{0} + a \implies a = 0$

$\implies f(x) = q(x)(x-r)$

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.

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

$d =$ "divisor"
$q =$ "quotient"
$r =$ "remainder"

Eg. $n=65$, $d=7$,

$$65 = \underline{9} \cdot 7 + \underline{2} \qquad 7 \nmid 65$$

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

$$91 = \underbrace{13}_{\text{quotient}} \cdot 7 + \underbrace{0}_{\text{remainder}} \qquad 7 \mid 91.$$

$$\begin{array}{r} 9 \\ 7\,\overline{)\,65} \\ \underline{63} \\ 2 \end{array}$$

d divides n $\quad (d \mid n) \iff n$ is a multiple of d, $n = qd\,(+0)$ ie. $r=0$.

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

<u>Theorem</u> (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. $F = \mathbb{Q}$, $\quad f(x) = x^3 - 2x - 3$, $d(x) = x^2 + x + 1$.

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

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

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

$$\begin{array}{r|l} & -\tfrac{1}{2}x \\ -2x-2 & x^2+x+1 \\ & x^2+x \end{array}$$

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

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

$$\begin{aligned}
100 &= 3\times \underline{27} + \underline{19} \\
27 &= 1\times \underline{19} + \underline{8} \\
19 &= 2\times \underline{8} + \underline{3} \\
8 &= 2\times 3 + 2 \\
3 &= 1\times 2 + \boxed{1} \\
2 &= 2\times 1 + 0
\end{aligned}$$

last nonzero remainder

$$\begin{aligned}
\gcd(100,27) = 1 &= 3-2 \\
&= 3-(8-2\times 3) \\
&= 3\times 3 - 8 \\
&= 3\times(19-2\times 8) - 8 \\
&= 3\times 19 - 7\times 8 \\
&= 3\times 19 - 7\times(27-19) \\
&= 10\times 19 - 7\times 27 \\
&= 10\times(100-3\times 27) - 37\times 27 \\
&= 10\times 100 - 37\times 27 \\
&= 1 \checkmark
\end{aligned}$$

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	$\boxed{1}$
*	*	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.

$$d(x) = \gcd(f(x), g(x)) \text{ is the largest monic polynomial such that } d(x) \mid f(x),\ d(x) \mid g(x).$$

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

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

$$f(x) = (x-1) g(x) + (-2x-2)$$
$$g(x) = \left(-\tfrac{1}{2}x\right)(-2x-2) + (1)$$
$$-2x-2 = (-2x-2)(1) + 0$$

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

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

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

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

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−1)②	1	$-x + 1$	$-2x - 2$
④ = ② + ½x③	$\tfrac{1}{2}x$	$-\tfrac{1}{2}x^2 + \tfrac{1}{2}x + 1$	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 (*)

$$1 = \left(\tfrac{1}{2}x\right) f(x) + \left(-\tfrac{1}{2}x^2 + \tfrac{1}{2}x + 1\right) g(\theta)$$
$$1 = \cancel{\left(\tfrac{1}{2}\theta\right) f(\theta)} + \left(-\tfrac{1}{2}\theta^2 + \tfrac{1}{2}\theta + 1\right) \overbrace{g(\theta)}^{\beta}$$

$$\frac{1}{\beta} = -\tfrac{1}{2}\theta^2 + \tfrac{1}{2}\theta + 1$$

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

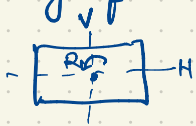
$[E : \mathbb{Q}] = 4$ with basis $\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$.

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)

$$\begin{tikzcd}
 & E \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}[\sqrt{2}] \arrow[dr, dash, "2"'] & \mathbb{Q}[\sqrt{5}] \arrow[d, dash, "2"] & \mathbb{Q}[\sqrt{10}] \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & G \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle V \rangle \arrow[dr, dash] & \langle H \rangle \arrow[d, dash] & \langle R \rangle \arrow[dl, dash] \\
 & 1 &
\end{tikzcd}$$

G Klein four-group



$VH = R$

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

$$\begin{array}{ccc} \mathbb{Q}[x] & \longrightarrow & \mathbb{Q}[\sqrt{2}] \subset \mathbb{R} \\ \Psi & & \Psi \\ f(x) & \longmapsto & f(\sqrt{2}) \end{array}$$

Evaluation maps are homomorphisms

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

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

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

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

homomorphism

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

$$\alpha = \underbrace{(a + b\sqrt{2})}_{\in \mathbb{Q}[\sqrt{2}]} 1 + \underbrace{(c + d\sqrt{2})}_{\in \mathbb{Q}[\sqrt{2}]} \sqrt{5}$$

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

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

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

Note: $\underbrace{[E : \mathbb{Q}]}_{4} = \underbrace{[E : \mathbb{Q}[\sqrt{2}]]}_{2} \times \underbrace{[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]}_{2}$.

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

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

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

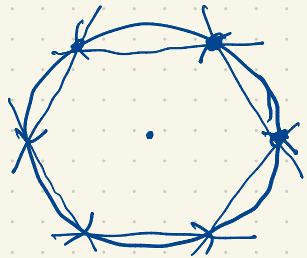
If $[K:F]=m$ and $[E:K]=n$ then we have
a basis $\{\alpha_1, \dots, \alpha_m\}$ we can choose a basis for K over F
so every $\alpha \in K$ can be uniquely written as
$$\alpha = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_m\alpha_m, \quad c_1, \dots, c_m \in F.$$
Every $\beta \in E$ can be written uniquely as
$$\beta = b_1\beta_1 + b_2\beta_2 + \cdots + b_n\beta_n, \quad b_j \in K$$
$\{\beta_1, \dots, \beta_n\}$ basis for E over K.

$$b_j = a_{1j}\alpha_1 + a_{2j}\alpha_2 + \cdots + a_{mj}\alpha_m, \quad a_{ij} \in F.$$
$$= \sum_{i=1}^{m} a_{ij}\alpha_i$$
$$\beta = \sum_{j=1}^{n} b_j\beta_j = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_{ij}\alpha_i\right)\beta_j = \sum_{i=1}^{m}\sum_{j=1}^{n} \underbrace{a_{ij}}_{\in F}\underbrace{\alpha_i\beta_j}_{E}$$

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.

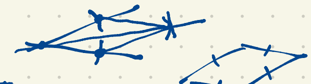
$E = \mathbb{Q}[\sqrt{2}, \sqrt{5}]$ cannot contain $\alpha = 2^{1/3}$.
If it did, we we would have
$$E \supseteq \mathbb{Q}[\alpha] \supseteq \mathbb{Q}$$
$$\underbrace{[E:\mathbb{Q}]}_{4} = \underbrace{[E:\mathbb{Q}[\alpha]]}_{?}\underbrace{[\mathbb{Q}[\alpha]:\mathbb{Q}]}_{3}$$
contradiction.

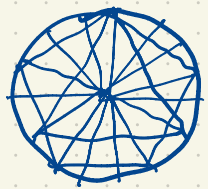
Straightedge and Compass Constructions



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

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





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.

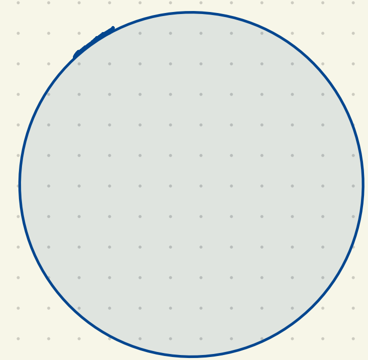
$2^m + 1 \qquad m = 2^k$

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 k^{th} roots

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

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^{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^{th} roots
- expressing antiderivatives 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 $\cancel{(a^b)^c}$

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

$\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\cdots}}}}$ 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: $\alpha = 1 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cdots}}}}}$ is the limit of the sequence $1,\ 1+\frac{1}{1},\ 1+\cfrac{1}{1+\frac{1}{1}},\ 1+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{1}}}, \dots$

$$1 = 1, \quad 1+\frac{1}{1} = 2, \quad 1+\cfrac{1}{1+\frac{1}{1}} = \frac{3}{2}, \quad 1+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{1}}} = \frac{5}{3}$$

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

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

$$\alpha = 1 + \frac{1}{\alpha}$$
$$\alpha^2 = \alpha + 1$$
$$\alpha^2 - \alpha - 1 = 0$$

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.

$$\mathbb{Q} \subset \mathbb{A} \subset \mathbb{C}$$

rational numbers

algebraic numbers

complex numbers

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

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

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

" — — — " — — — — " — — — " ab is rational? eg $\sqrt{2} \cdot \sqrt{2} = 2$.

or $\sqrt{2} \cdot \frac{1}{\sqrt{2}} = 1$