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. □

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 $1, \pi, \pi^2, \pi^3, \ldots$ 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?

$1, \alpha, \alpha^2, \ldots, \alpha^n$ 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 $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{Q}[x]$.

If $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ 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 $\deg 0 = -\infty$.

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

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

If $g(x) = x^3-4x-11$ then $0g(x) = 0$

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

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

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

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

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

$\alpha = \sqrt{2}+\sqrt{5}$ 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.

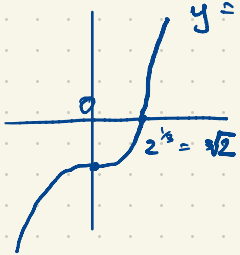
In case (i), $x^4 - 10x^2 + 1 = (x+a)(x^3 + bx^2 + cx + d)$, $ad = 1$, $a = d = \pm 1$.
In this case $m(x)$ has ± 1 as a root but $m(1) = -8 = m(-1)$, a contradiction.

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 $7 \in \mathbb{Z}$.
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 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 $2^{1/3} \notin \mathbb{Q}$ essentially by Euclid's argument.



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 {factor / divisor} 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 $f(r) = (r-r)q(r) = 0$.
What about the converse? By the Division Algorithm, $f(x) = q(x)(x-r) + a(x)$, $\deg a(x) < \deg(x-r)$
($\deg a(x) = 0$ or $-\infty$; $\deg(x-r) = 1$)
If r is a root of $f(x)$ then $f(r) = 0 = q(r)\underbrace{(r-r)}_{0} + a \Rightarrow a = 0$
$\Rightarrow f(x) = q(x)(x-r)$
$a(x) = a$ = 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 $n = qd + r$, $0 \leq r < d$.

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

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

$65 = 8 \cdot 7 + 9$

$91 = 13 \cdot 7 + 0$ $\quad 7 \mid 91$.

(quotient, remainder)

$$\begin{array}{r|l} & 9 \\ 7 & 65 \\ & 63 \\ \hline & 2 \end{array}$$

d **divides** n $(d \mid n)$ $\iff$ 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 $\mathbb{Z}[x]$.

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

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

$$\begin{array}{r|l} & x - 1 \\ x^2+x+1 & x^3 \quad -2x - 3 \\ & x^3 + x^2 + x \\ \hline & -x^2 - 3x - 3 \\ & -x^2 - x - 1 \\ \hline & -2x - 2 \end{array}$$

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

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

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 $a, b \in \mathbb{Z}$

$100 = 3 \times 27 + 19$

$27 = 1 \times 19 + 8$

$19 = 2 \times 8 + 3$

$8 = 2 \times 3 + 2$

$3 = 1 \times 2 + \boxed{1}$ ← $\gcd(100, 27) = 1$ (last nonzero remainder)

$2 = 2 \times 1 + 0$

Continue Monday

$1 = 3 - 2$

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

$= 3 \times 3 - 8$

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

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

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

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

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

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

$= 1$ ✓

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

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

$\gcd(100, 27) = 1$

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

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. $f(x) = x^3 - 2x - 3$

$g(x) = x^2 + x + 1$

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

$$g(x) = (-\tfrac{1}{2}x)(-2x-2) + (1)$$

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

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

$$\begin{aligned} 1 &= g(x) + (\tfrac{1}{2}x)(-2x-2) \\ &= g(x) + (\tfrac{1}{2}x)\big(f(x) - (x-1)g(x)\big) \\ &= (\tfrac{1}{2}x)f(x) + (1 - \tfrac{1}{2}x^2 + \tfrac{1}{2}x)g(x) \end{aligned}$$

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

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)②	1	$-x + 1$	$-2x - 2$
④ = ② + $\tfrac{1}{2}x$③	$\tfrac{1}{2}x$	$-\tfrac{1}{2}x^2 + \tfrac{1}{2}x + 1$	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 (*) $\quad 1 = (\tfrac{1}{2}x)f(x) + (-\tfrac{1}{2}x^2 + \tfrac{1}{2}x + 1)g(\theta)$ $\quad \beta$

$$1 = (\tfrac{1}{2}\theta)f(\theta) + (-\tfrac{1}{2}\theta^2 + \tfrac{1}{2}\theta + 1)\,g(\theta)$$

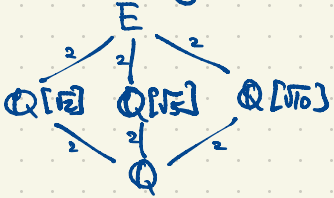
$\frac{1}{\beta} = -\tfrac{1}{2}\theta^2 + \tfrac{1}{2}\theta + 1$

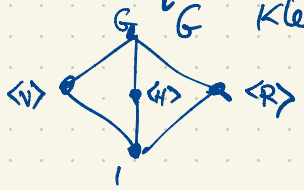
$E = \mathbb{Q}[\sqrt{2},\sqrt{5}] = \{a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10} : a,b,c,d \in \mathbb{Q}\}$

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

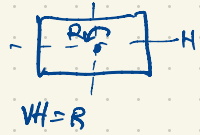
E has subfields $\mathbb{Q}$, E, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{10}]$

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





Klein four-group



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

$4 \qquad 2 \times 2$

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

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

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

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. $[\mathbb{C}:\mathbb{Q}] = [\mathbb{C}:\mathbb{R}][\mathbb{R}:\mathbb{Q}]$

$\infty \qquad 2 \qquad \infty$

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

$\beta = b_1\beta_1 + b_2\beta_2 + \cdots + b_n\beta_n$, $b_i \in K$

$\{\beta_1, \dots, \beta_n\}$ basis for E over K.

$$b_j = a_{1j}\alpha_1 + a_{2j}\alpha_2 + \cdots + a_{mj}\alpha_m, \quad a_{ij} \in F.$$

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

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

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

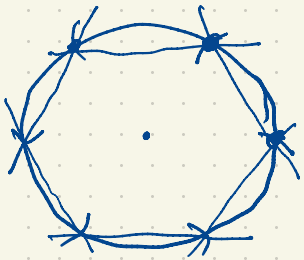
$$E \supseteq \mathbb{Q}[\alpha] \supseteq \mathbb{Q}$$

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

$4 \qquad ? \qquad 3$

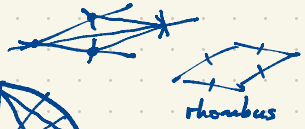
contradiction.

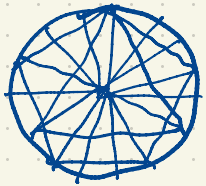
Straightedge and Compass Constructions



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.

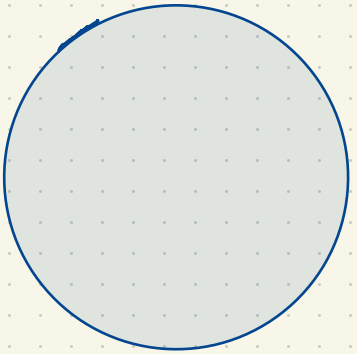
$2^m + 1 \qquad m = 2^k$

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 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^{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 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 ~~$(a^b)^c$~~

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

$\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\cdots}}}}$ is the limit of a sequence $\sqrt{2}, \sqrt{2}^{\sqrt{2}}, \sqrt{2}^{\sqrt{2}^{\sqrt{2}}}, \sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}}}}, \ldots$

i.e. the sequence $a_1, a_2, a_3, a_4, \ldots$ 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 $1,\ 1+\frac{1}{1},\ 1+\cfrac{1}{1+\frac{1}{1}},\ 1+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{1}}}, \ldots$

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

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

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

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

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

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

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

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 $a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$.

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

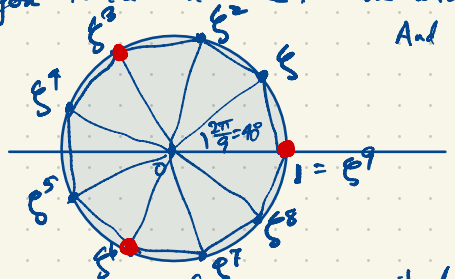
This is a nonconstructive proof.

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

Liouville's constant $\sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0.110001000000000000000001000\ldots$

This was the first known explicit transcendental number.

Regular 9-gon in the unit circle.



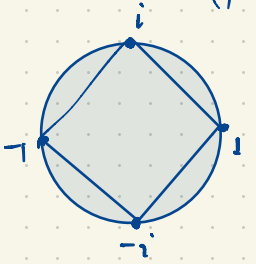
We will show that this figure is not constructible using straightedge and compass.

And so it follows that a $120°$ angle cannot be trisected using " " " ".

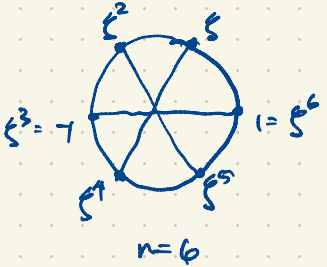
You can't trisect $60°$ angle

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 $\mathbb{C}$.



$n=4$

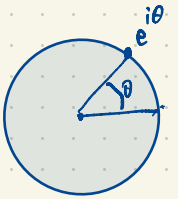


$n=6$

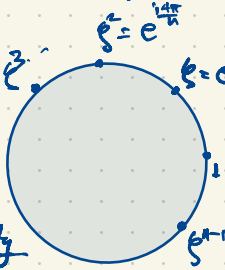
De Moivre's formula (see "review" on complex numbers linked on the course website)

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

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 $x^n - 1 = (x-1)(x-\xi)(x-\xi^2)\cdots(x-\xi^{n-1})$



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

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

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

$\{1, \xi, \xi^2, \cdots, \xi^{n-1}\}$ is a multiplicative cyclic group. $\xi^j \cdot \xi^k = \xi^{j+k}$ (exponents mod n).

Any element in this group generates a subgroup. If ξ^j generates the whole group, it's called a primitive n^{th} root of unity.

Eg. for $n=9$, the 9^{th} roots of unity form a cyclic group $\langle \xi \rangle = \{1, \xi, \xi^2, \cdots, \xi^8\}$, $\xi^9 = 1$

where $\xi = e^{2\pi i/9}$ $\qquad \langle \xi^3 \rangle = \{1, \xi^3, \xi^6\}$

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

The 9 ninth roots of unity are the roots of

$$x^9 - 1 = (x-1)(x^8 + x^7 + x^6 + \cdots + x + 1)$$
$$= (x^3-1)(x^6+x^3+1) = (x-1)(x^2+x+1)(x^6+x^3+1)$$

(irreducible factors in $\mathbb{Q}[x]$)

root: 1 (the 1st root of unity)

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

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

$\phi(9) = 6$

The 9^{th} roots of unity add up to 0:

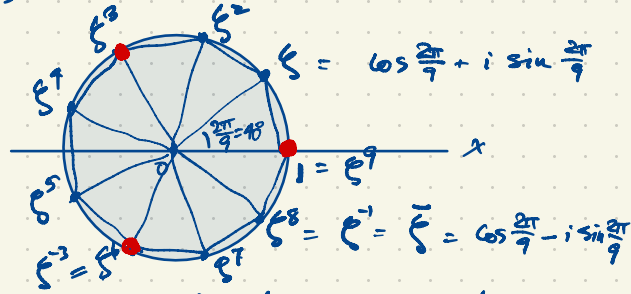
$$1 + \xi + \xi^2 + \cdots + \xi^8 = 0$$

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

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

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

is algebraic of degree 3



$1 + \xi^3 + \xi^6 = 0 \Rightarrow \xi^3 + \xi^6 = -1$

$\xi^3 + \xi^{-3} = -1$

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

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

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

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

$= -1 + 3\alpha$

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

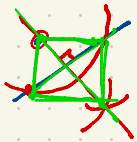
The min. poly. of α is $x^3 - 3x + 1$.

Now you can do HW2 #5.

Straightedge & Compass Constructions

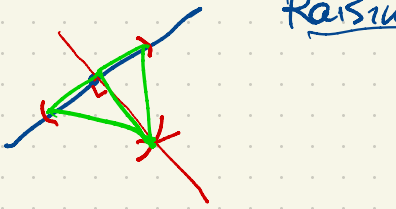
Bisecting an angle

Rhombus (parallelogram with sides of equal length)

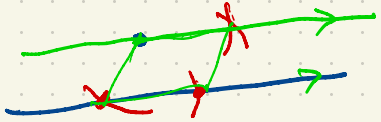


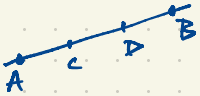
Dropping a perpendicular

Raising a perpendicular



Constructing a parallel line



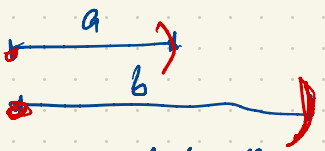


Trisecting a line segment

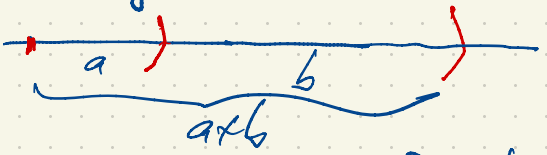
(or divide a line segment into n equal segments for any n)

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

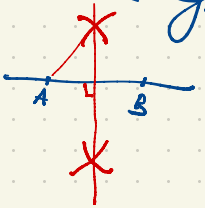
Given a line segment, multiply its length by any rational number.

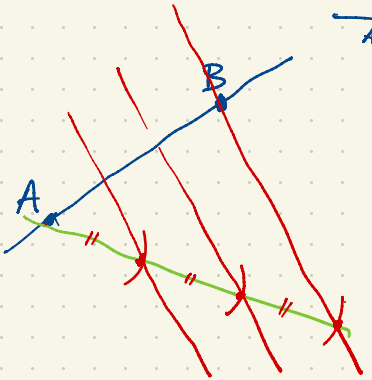


Add lengths:

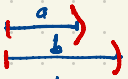


Bisect line segment





Can we multiply the lengths of two line segments?

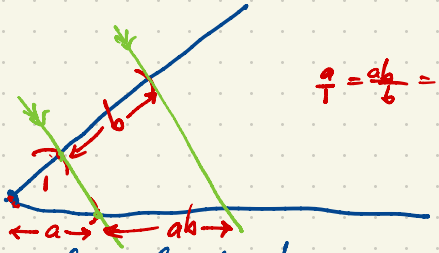


Given line segments of length a, b, can we construct a line segment of length ab?

First specify a unit length: 

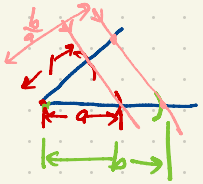
Now:

Draw any angle (not 0° or 180°)

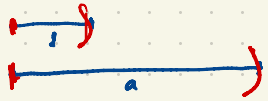


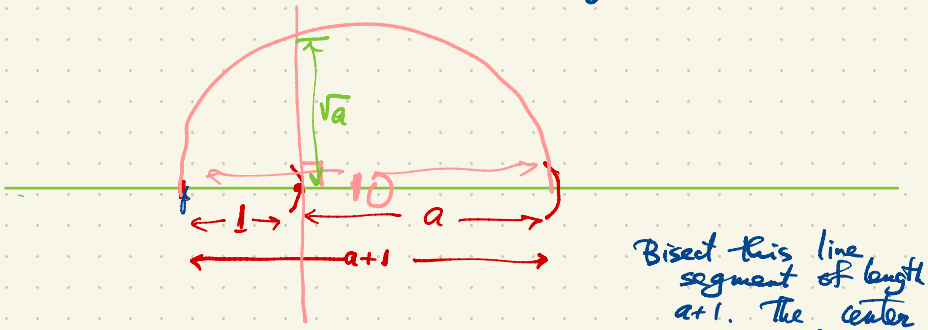
$\frac{a}{1} = \frac{ab}{b} = \frac{a+ab}{1+b}$

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

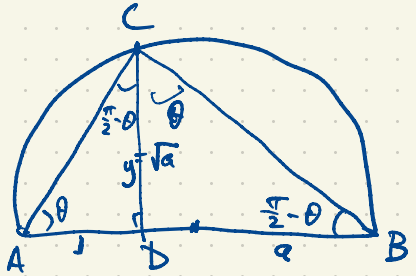


Can we find a line segment of length $\sqrt{a}$, given line segments of length 1 and a ?





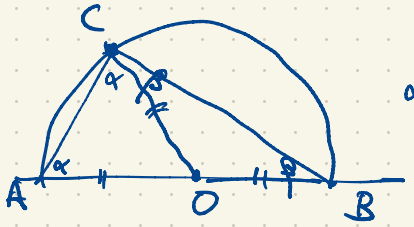
Bisect this line segment of length $a+1$. The center is at a point we'll call O.
Construct the semicircle centered at O of radius equal to the distance shown.



The three triangles in this picture are similar:

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

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



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

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

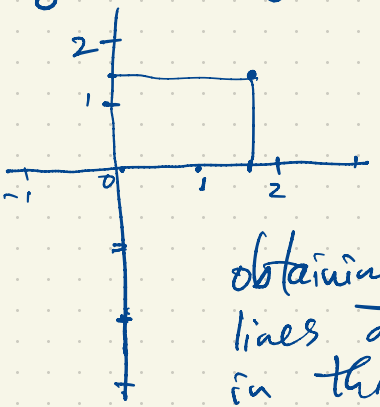
What can be constructed using straightedge and compass only?

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.

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

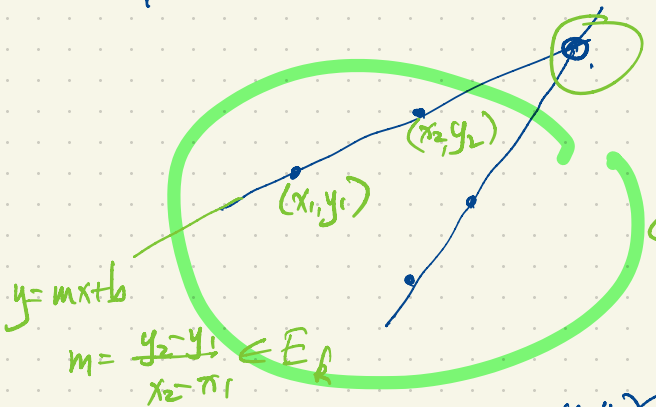


Any point in $\mathbb{Q}^2 = \{(x,y) : x,y \in \mathbb{Q}\}$ is then constructible.

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.

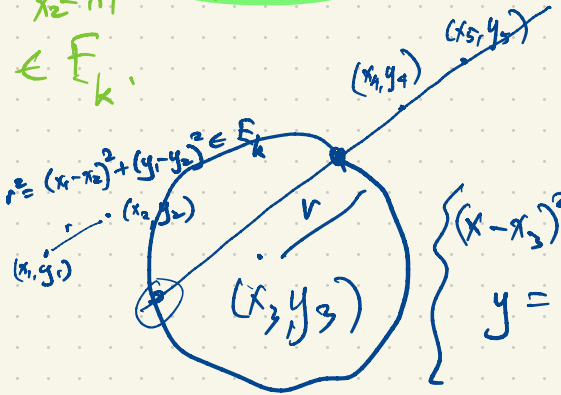
At the start, all points in our construction are in $\mathbb{Q}^2$.
Let E_k be the field generated by all coordinates of points up to step k.

$E_0 = \mathbb{Q}$.
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



new point will have coordinates also in E_k
$\Rightarrow E_{k+1} = E_k$.

coordinates in E_k.

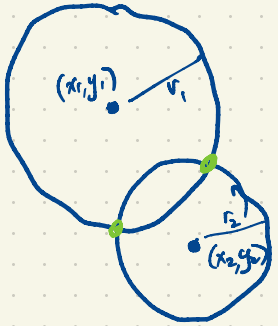


If in step k we are intersecting a previous line with a previous circle, the new points (x, y) will have coordinates in E_{k+1}, where $[E_{k+1} : E_k] = 1$ or 2.

$$\begin{cases} (x - x_3)^2 + (y - y_3)^2 = r^2 & x_3, y_3, r^2 \in E_k \\ y = mx + b & m = \frac{y_5 - y_4}{x_5 - x_4} \in E_k \\ & b \in E_k \end{cases}$$

If in step k we are intersecting two previous circles

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



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

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

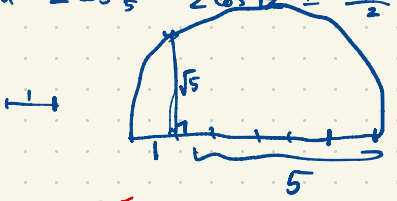
$$\iff \begin{cases} x^2 - 2x_1x + x_1^2 + y^2 - 2y_1y + y_1^2 = r_1^2 \\ 2(x_1-x_2)x + x_2^2 - x_1^2 + 2(y_1-y_2)y + y_2^2 - y_1^2 = r_2^2 - r_1^2 \end{cases}$$

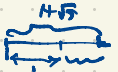
$$\boxed{*}x + \boxed{*}y = \boxed{*}$$

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

To construct a regular pentagon using straightedge and compass,

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





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

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

$\mathbb{F}_9 = \{a+bi : a,b \in \mathbb{F}_3\}$ $\quad i = \sqrt{-1} = \sqrt{2}$ $\quad -1 = 2$

$[\mathbb{F}_9 : \mathbb{F}_3] = 2$ with basis $\{1, i\}$ $\quad \cdots = -10 = -7 = -4 = -1 = 2 = 5 = 8 = \cdots$

$\mathbb{F}_9 = \{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$, $2 = -1$

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

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

$x^2+x+1 = (x-1)(x-1)$ roots $\frac{-1 \pm \sqrt{1-4}}{2} = \frac{-1 \pm \sqrt{-3}}{2} = -\frac{1}{2} = 1$ (a double root)

$= (x-1)^2$

$= x^2-2x+1$ ✓

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.

$x^2+x = x(x+i)$ has roots $0, 2$ in $\mathbb{F}_3 \subset \mathbb{F}_9$.

$\frac{-1 \pm \sqrt{1}}{2} = \frac{-1 \pm 1}{2} = 0$ or $-1 = 2$

Test: only on material up to here

Field Characteristic

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

$0, 1 \in K \Rightarrow$ $1+1=2 \in K$

$1+1+1=3 \in K$

$1+1+1+1=4 \in K$

$1+1+1+1+1=5 \in K$

$1+1+1+1+1+1=6 \in K$

$1+1+1+1+1+1+1=7 \in K$

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 $\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$ 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.