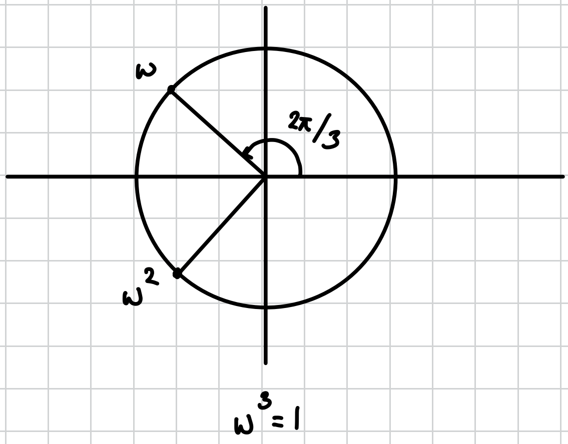
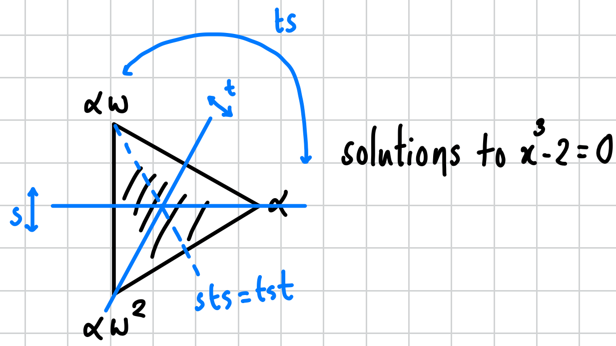
0. What is Galois Theory

Example: Symmetries of the solutions to $x^3 - 2 = 0$.

Let $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$





These solutions have "geometrical" symmetry,

i.e. s, t, tst (reflections) $\quad ts, (ts)^2, (ts)^3 = 1_G$ (rotations)

These are NOT the symmetries we want.

Fields

Definition Field

A **field** is a set $\mathbb{F}$ together with binary operations

addition: $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$, $(\alpha, \beta) \mapsto \alpha + \beta$

multiplication: $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$, $(\alpha, \beta) \mapsto \alpha\beta$

satisfying the following axioms

Commutativity: $\forall \alpha, \beta \in \mathbb{F}$,

$$\alpha + \beta = \beta + \alpha \qquad \alpha\beta = \beta\alpha$$

Associativity: $\forall \alpha, \beta, \gamma \in \mathbb{F}$,

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma \qquad \alpha(\beta\gamma) = (\alpha\beta)\gamma$$

Identity elements: $\exists\, 0, 1 \in \mathbb{F}$, $0 \neq 1$ such that for all $\mathbb{F}$,

$$\alpha + 0 = \alpha \qquad \alpha 1 = \alpha$$

Inverses: $\forall \alpha \in \mathbb{F}$, $\exists -\alpha \in \mathbb{F}$ such that

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

$\forall \alpha \in \mathbb{F}$, $\exists\, \alpha^{-1} \in \mathbb{F}$ such that

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

Distributivity: $\forall \alpha, \beta, \gamma \in \mathbb{K}$, we have

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

Subfield

Definition

A **subfield** of a field is a subset that is also a field under the same $+, \times$

Example: $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Rings Recap

Definition Abelian Groups

An **Abelian** (commutative) **group** R is a set with a binary operation

$$+: R \times R \to R$$
$$(a,b) \mapsto a+b$$

such that

(0) $a+b = b+a \quad \forall a,b \in R$

(1) $a+(b+c) = (a+b)+c$

(2) $\exists\, 0 \in R$ s.t $0+a = a+0 \quad \forall a \in R$

(3) $\forall a \in R, \exists (-a) \in R$ s.t $a+(-a) = (-a)+a = 0$

Notation: We write $a+(-b) = a-b$

Definition of a ring

Definition Ring

A **ring** R is a set with 2 binary operations

addition	multiplication
$R \times R \to R;$	$R \times R \to R;$
$(a,b) \mapsto a+b$	$(a,b) \mapsto a \times b$

satisfying following axioms

i) $(R,+)$ is an Abelian group

ii) $(a\times b)\times c = a \times (b \times c) \quad \forall a,b,c \in R$

iii) $a \times (b+c) = a\times b + a \times c \quad \forall a,b,c \in R$

$(a+b)\times c = a \times c + b \times c \quad \forall a,b,c \in R$

Notation: $a \times b$ is represented by ab

Commutative Ring

Definition Commutative Ring

A ring is commutative if $\forall a, b \in R$,

$$a \times b = b \times a$$

i.e. multiplication is commutative

Subrings

Definition Subring

Let R be any ring $(+, \times)$, let $S \subseteq R$ be any subset

We say S is called a subring of R if:

(a) $0 \in S$ (identity)

(b) $a, b \in S \implies -a \in S,\ a+b \in S,\ a \times b \in S$ (closure)

Ring Homomorphism

Definition Ring Homomorphism

Let R, S be any 2 rings. A function

$$\alpha : R \to S$$

is a ring homomorphism if $\forall a, b \in R$

i) $\alpha(a \underset{R}{+} b) = \alpha(a) \underset{S}{+} \alpha(b)$

ii) $\alpha(a \underset{R}{\times} b) = \alpha(a) \underset{S}{\times} \alpha(b)$

If R and S are rings with identity 1 and

$$\alpha(1) = 1$$

then α is a unital ring homomorphism

Important!

Let R and S are rings with multiplicative identity $1_R \in R$ and $1_S \in S$

If $\alpha: R \to S$ is an onto homomorphism (or isomorphism) then

$$\alpha(1_R) = 1_S$$

Smallest subfields

Definition

$F \subseteq \mathbb{C}$ a subfield and $\beta \in \mathbb{C}$.

Write $F(\beta)$ to mean the smallest subfield of $\mathbb{C}$ containing F and β

Here the smallest means if F' is any subfield of $\mathbb{C}$ containing F and β, then

$$F(\beta) \subseteq F'$$

Example:

Can also consider $F(\beta_1, \beta_2)$ etc ... so that we have $\mathbb{Q}(\alpha, \omega)$

Then $\alpha, \omega \in \mathbb{Q}(\alpha, \omega)$

$$\Longrightarrow \alpha \times \omega = \alpha\omega, \ \alpha \times \omega \times \omega = \alpha\omega^2 \in \mathbb{Q}(\alpha, \omega)$$

i.e. $\mathbb{Q}(\alpha, \omega)$ contains the solutions to $x^3 - 2 = 0$

Exercise: $\mathbb{Q}(\alpha, \omega)$ is the smallest subfield of $\mathbb{C}$ containing these solutions

Loosely a symmetry of the solutions to $x^3 - 2 = 0$ is a symmetry of $\mathbb{Q}(\alpha, \omega)$ that respects the $+, \times$

Example: Consider $\mathbb{Q}(\alpha, \omega)$ and $\mathbb{Q}(\alpha, \omega^2)$

Then: $\alpha, \omega \in \mathbb{Q}(\alpha, \omega) \Longrightarrow \alpha, \omega \times \omega = \omega^2 \in \mathbb{Q}(\alpha, \omega)$

$$\Longrightarrow \mathbb{Q}(\alpha, \omega^2) \subseteq \mathbb{Q}(\alpha, \omega)$$

$$\alpha, \omega^2 \in \mathbb{Q}(\alpha, \omega^2) \Longrightarrow \alpha, \omega^2 \times \omega^2 = \omega^4 \in \mathbb{Q}(\alpha, \omega^2)$$

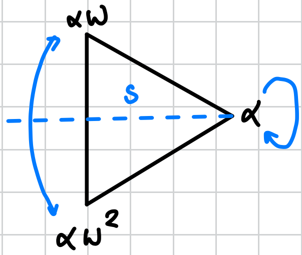
$$\Longrightarrow \mathbb{Q}(\alpha, \omega) \subseteq \mathbb{Q}(\alpha, \omega^2)$$

Thus $\exists$ a symmetry $\mathbb{Q}(\alpha, \omega) \longrightarrow \mathbb{Q}(\alpha, \omega^2)$

which sends $\alpha \mapsto \alpha$ and $\omega \mapsto \omega^2$

Then $\alpha\omega \mapsto \alpha\omega^2$

$$\alpha\omega^2 = \alpha\omega\omega \longmapsto \alpha\omega^2\omega^2 = \alpha\omega^4$$
$$= \alpha\omega$$

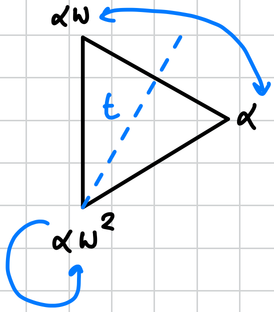


Try at home

$$\mathbb{Q}(\alpha,\omega) = \mathbb{Q}(\alpha\omega,\omega^2)$$

$\implies tst,\ ts,\ (ts)^2$ etc all symmetries

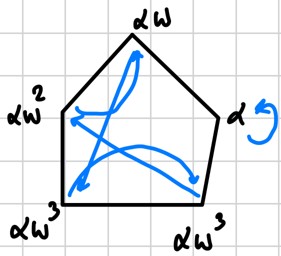
But Galois Theory not geometry



Example: $x^5 - 2 = 0$

$$\alpha = \sqrt[5]{2}$$

$$\omega = \frac{\sqrt{5}-1}{4} + \frac{\sqrt{2}\sqrt{5+\sqrt{5}}}{4}\,i$$



Zero Divisors

Definition Zero Divisors

Let R be a ring and $R \neq \{0\}$

An element $a \in R$ is a zero divisor if for some $b \in R\setminus\{0\}$, $b \neq 0$

$$ab = 0 \text{ or } ba = 0$$

Integral Domains

Definition Integral Domains

An integral domain is a commutative ring with identity $1 \in R$ s.t

$$ZD = \{0\}$$

that is has NO non-trivial non-zero. Equivalently

$$NZD(R) = R\setminus\{0\}$$

Example

$R = \mathbb{Z}$, $ZD(R) = \{0\} \implies$ Integral Domain

Remark: For any ring R, the condition $ZD(R) = \{0\}$ is equivalent to either of

i) $\forall a, b \in R \setminus \{0\}$, we have $ab \neq 0$

ii) $\forall a, b \in R$, the equality $ab = 0 \implies a = 0$ or $b = 0$

Example: $\mathbb{Z}_6$ NOT an ID

1 Rings of Polynomials

Let R be any commutative ring with identity $1 \in R, 1 \neq 0$

Let x be a formal symbol $(x \notin R)$

A polynomial in x over R is a formal expression

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

where $n \in \mathbb{N}^0 = \mathbb{N} \cup \{0\}$ and $a_0, \ldots, a_n \in R$.

a_i is the co-efficient of x^i

Conventions

(a) $x^0 = 1$ and $x^1 = x$

(b) We can miss terms $a_i x^i$ with $a_i = 0$ (0 coefficient)

<u>For example</u>: $1 + \cancel{0x^1} + 2x^2 = 1 + 2x$

(c) We abbreviate $1x^i = x^i$

(d) A polynomial of form $ax^0 = a1 = a$ is called a constant polynomial

(e) Consider 2 polynomials

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

$$g = b_0 + b_1 x + \cdots + b_m x^m$$

When $m = n$: $f = g \iff a_0 = b_0, \ a_1 = b_1, \ \ldots, \ a_n = b_n$

When $n > m$, apply convention (b)

$$g = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m + 0x^{m+1} + \cdots + 0x^n$$

$$\Longrightarrow b_{m+1} = 0, \ \ldots, \ b_n = 0$$

Similar for $n > m$. Then for equality, we have

if $m \geq n$ $\quad f = g \iff a_0 = b_0, \ a_1 = b_1, \ \ldots \ a_n = b_n, \ b_{n+1} = \cdots = b_m = 0$

if $m \leq n$ $\quad f = g \iff a_0 = b_0, \ a_1 = b_1, \ \ldots \ a_n = b_n, \ a_{m+1} = \cdots = a_n = 0$

Ring of Polynomials

Definition

Let R be any commutative ring with identity $1 \in R$, $1 \neq 0$

Denote the set of all polynomials over R by

$$R[x]$$

Define addition and multiplication

Addition: $(+)$

$\forall f, g \in R[x]$

$$f = a_0 + a_1 x + \cdots + a_n x^n$$
$$g = b_0 + b_1 x + \cdots + b_m x^m \qquad m, n \in \mathbb{N}^0$$

$$f + g = c_0 + c_1 x + \cdots + c_\ell x^\ell \quad , \quad \ell = \max\{n, m\}$$

$$c_i = \begin{cases} a_i + b_i & \text{if } i \leq \min\{m, n\} \\ a_i & \text{if } m < i \leq n \\ b_i & \text{if } n < i \leq m \end{cases} \qquad (c_0 = a_0 + b_0)$$

By convention (e), assume $n = m$. If $m \neq n$, then append 0 terms to the "shorter polynomial

$$f + g = (a_0 + b_0)x^0 + (a_1 + b_1)x^1 + \cdots + (a_n + b_n)x^n$$

Multiplication: $(\times)$

$$f \times g = (a_0 + a_1 x + \cdots + a_n x^n) \times (b_0 + b_1 x^1 + \cdots + b_m x^m) = d_0 + d_1 x + \cdots + d_{n+m} x^{n+m}$$

where for $0 \leq k \leq m+n$

$$d_k = \sum_{\substack{i,j \\ i+j=k}} a_i b_j$$

Note that

$$f \times g = (a_0 x^0 + a_1 x^1 + \cdots + a_n x^n)(b_0 x^0 + b_1 x^1 + \cdots + b_m x^m)$$
$$= a_0 b_0 x^0 + (a_0 b_1 + a_1 b_0)x^1 + \cdots + a_n b_m x^{n+m}$$

Proposition Ring of Polynomials

Let R be any commutative ring with identity $1 \in R, 1 \neq 0$

Then
$$(R[x], +, \times)$$
is a commutative ring with an identity.

Theorem

Let R be an integral domain

Then $R[x]$ is an integral domain, i.e. $\forall f, g \in R[x] \setminus \{0\}$
$$fg \neq 0 \quad \text{and} \quad \deg(fg) = \deg(f) + \deg(g)$$

Example: Non-example

$R = \mathbb{Z}_6$, then $(3x+1)(2x+1) = 5x+1$

Example: R commutative ring with $1 \in R$ and $c \in R$ and define
$$\varepsilon_c : R[x] \longrightarrow R$$
by $\varepsilon_c(a_n x^n + \cdots + a_1 x + a_0) = a_n c^n + \cdots + a_1 c + a_0$

Then ε_c is a ring homomorphism
$$\varepsilon_c(f+g) = \varepsilon_c(f) + \varepsilon_c(g)$$
$$\varepsilon_c(fg) = \varepsilon_c(f)\,\varepsilon_c(g)$$

Division Algorithm

Theorem Division algorithm

Let $f, g \in R[x]$ s.t
$$g = b_m x^m + \cdots + b_1 x + b_0 \quad (b_i \in R)$$
with b_m having an inverse in R under $\times$

Then $\exists$ unique $q, r \in R[x]$ s.t
$$f = qg + r \qquad \deg(r) < \deg(g)$$

Remark:

If $R =$ a field then the condition on g is just $g \neq 0$

Roots and irreducibility

If $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[X]$

and $c \in R$, then c is a root of f when:

$$a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0 = 0 \quad (\text{in } R)$$

Example: x^2+1 is an element of $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$

Has no roots in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

Theorem Factor Theorem

$f \in R[X]$ has a root $c \in R$ iff

$$f = (x-c)g \quad \text{where } g \in R[x]$$

Theorem

$f \in R[X]$ where R is an integral domain.

Then f has atmost $\deg(f)$ roots in R

Example: $x^2 + 3x + 2 \in \mathbb{Z}_6[x]$ not an ID

$$= (x-1)(x-2) \Longrightarrow x = 1 \text{ or } x = 2$$

and $(x-1)(x-2) = 3 \times 2$ (i.e. $x = 4$) (i.e. 4 roots)

$(x-1)(x-2) = 4 \times 3$ (i.e. $x = 5$)

Definition

Let $f, g \in R[x]$

A non-trivial factorization of

$$f = gh$$

with $g, h \in R[x]$ and $\deg(g), \deg(h) \geq 1$ (equivalently $\deg(g), \deg(h) < \deg(f)$)

Definition reducible/irreducible

Call f **reducible** over field F if $\exists$ a non-trivial factorization

Otherwise F is **irreducible**

Example: $x^2+1 = (x-i)(x+i)$ in $\mathbb{C}[X]$

- reducible over $\mathbb{C}$
- x^2+1 irreducible over $\mathbb{Q}, \mathbb{R}$

Example: $f = ax+b \quad (a, b \in F)$

f is irreducible over F

For if $f = gh$ with $\deg(g), \deg(h) \geq 1$

$$\deg(f) = \deg(g) + \deg(h) \geq 1+1 \quad \divideontimes$$

Theorem Fundamental theorem of algebra

If $f \in \mathbb{C}[X]$ is non-constant, then f has a root in $\mathbb{C}[X]$

Consequence:

If $\deg(f) \geq 2$ then f has a root $c \in \mathbb{C}$ hence

$$f = (x-c)g \in \mathbb{C}[x]$$

i.e. f reducible over $\mathbb{C}$

$\Longrightarrow$ only linear polynomials irreducible over $\mathbb{C}$

Example:

Irreducible over F $\neq$ having no roots in F

f has no roots in F $\not\Longrightarrow$ f is irreducible over F

eg: $x^4+2x^2+1 \in \mathbb{Q}[X]$

$= (x^2+1)^2$ reducible over $\mathbb{Q}$

and clearly no roots in $\mathbb{Q}$

f irreducible over F $\not\Longrightarrow$ f has no roots in F

eg: $ax+b \in F[X]$ irreducible over F

but has root $-\frac{b}{a} = -ba^{-1} \in F$

Proposition

if $f \in F[x]$ with $\deg(f) \leq 3$

f has no roots in $F \iff f$ irreducible over F

Proof: both ways contrapositive

$(\Rightarrow)$: Suppose f has a root. We will show f is not irreducible.

$\exists\, a \in F$ s.t $f(a) = 0$. Let us divide by $(x-a)$ with a remainder

$$f = (x-a)q + r \text{ where } \underbrace{\underbrace{r=0}_{\text{zero const}} \text{ or } \underbrace{r \neq 0 \text{ but } \deg(r) < 1}_{\text{non-zero const}}}_{r \text{ is a const}}$$

$$0 = f(a) = 0q + r \implies r = 0$$

$$2,3 = \deg f = \underbrace{\deg(x-a)}_{1} + \deg q = 1,2 \;\Big|\implies f \text{ is not irreducible}$$

$(\Leftarrow)$: Suppose f is not irreducible. Need to prove f has a root

So $f = uv$, u, v are non-constant polynomials

$$2,3 = \deg(f) = \underset{\substack{\vee\mid \\ 1}}{\deg(u)} + \underset{\substack{\vee\mid \\ 1}}{\deg(v)} \implies \deg(u) = 1 \text{ or } \deg(v) = 1$$

Suppose $\deg u = 1 \implies u = cx + d$, where $c \neq 0 \implies c^{-1} \in F$

$$f = (cx+d)v = c(x + c^{-1}d) \implies x = c^{-1}d, \text{ then } x \text{ is a root}$$

Similar for $\deg v = 1$

■

Field $\mathbb{Z}_p$

We need another field to play with.

Seen that $(\mathbb{Z}_n, +, \times)$ a ring

$$\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$$

If $n = p$ prime, then $\mathbb{Z}_p$ a field

[hint: if $k \in \mathbb{Z}_p$ with $k \neq 0$, then $\exists\, a \in \mathbb{Z}_p$ s.t

$$ak \equiv 1 \pmod{p}$$

i.e. $ak = 1$ in $\mathbb{Z}_p$]

Notation: Write $\mathbb{F}_p$ from now on, instead of $\mathbb{Z}_p$

If $n \neq$ prime, then $\mathbb{Z}_p$ not a field

(eg: $\mathbb{Z}_6$ with $2, 3 \in \mathbb{Z}_6$ when $2 \times 3 = 0 \in \mathbb{Z}_6$ but a field is an ID)

We have the sequence:

$$\mathbb{F}_2, \mathbb{F}_3, \mathbb{Z}_4, \mathbb{F}_5, \mathbb{Z}_6, \mathbb{F}_7, \mathbb{Z}_8, \mathbb{Z}_9, \mathbb{Z}_{10}, \mathbb{F}_{11}$$

(We will see that $\exists$ fields $\mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_9, \dots$ but these are not $\mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_9$)

Example: $x^4 + x + 1 \in \mathbb{F}_2[x]$

Claim: This is irreducible over $\mathbb{F}_2$

Check for roots $\left.\begin{array}{l} 0^4 + 0 + 1 = 1 \\ 1^4 + 1 + 1 = 1 \end{array}\right\} \Rightarrow$ no roots in $\mathbb{F}_2$.

This gives that the only possible factorisation is as a product of 2 quadratics

Moreover these 2 quadratics are themselves irreducible over $\mathbb{F}_2$

The quadratics over $\mathbb{F}_2$ are

x^2	x^2+1	x^2+x	x^2+x+1
$x\,x$	$(x+1)^2$	$x(x+1)$	$\left.\begin{array}{l} 0^2+0+1 \\ 1^2+1+1 \end{array}\right\}$ no roots in $\mathbb{F}_2$ and deg ≤ 3 $\Rightarrow$ irreducible over $\mathbb{F}_2$

All we have left is x^2+x+1 but

$$x^4+1 \neq (x^2+x+1)^2$$

$\Rightarrow$ irreducible over $\mathbb{F}_2$

Irreducibility over $\mathbb{Q}$

Lemma Gauss Lemma

A polynomial with $\mathbb{Z}$ coefficients can be factorized into 2 factors with $\mathbb{Z}$ coefficients

$$\Updownarrow$$

it can be factorized into 2 factorized into 2 factors with $\mathbb{Q}$ coefficients

Theorem Eisenstein irreducibility

Let
$$f = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 + c_0$$
with the $c_i \in \mathbb{Z}$. Suppose also that $\exists$ a prime p s.t

(i) p divides $c_0, c_1, \dots, c_{n-1}$

(ii) $p \nmid c_n$

(iii) $p^2 \nmid c_0$

Then f is irreducible over $\mathbb{Q}$.

__Proof__: (via contradiction)

Suppose $f = gh$ with $g, h \in \mathbb{Q}[x]$.

By Gauss Lemma, can assume that
$$g = a_r x^r + \cdots + a_1 x + a_0$$
$$h = b_s x^s + \cdots + b_1 x + b_0$$
with $a_i, b_i \in \mathbb{Z}$. Then
$$c_0 = a_0 b_0$$
$$c_1 = a_0 b_1 + a_1 b_0$$
$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$
$$\vdots$$
$$c_i = a_0 b_i + \cdots + a_i b_0$$
$$\vdots$$
$$c_n = a_r b_s$$

$p \mid c_0 \Rightarrow p \mid a_0 b_0$

$\Rightarrow p \mid a_0$ or $p \mid b_0$

But $p^2 \nmid c_0 \Rightarrow$ can't have both.

Assume $p \mid a_0$ but $p \nmid b_0$

Now $p \mid c_1 \Rightarrow p \mid c_1 - a_0 b_1$

$\Rightarrow p \mid a_1 b_0$

$\Rightarrow p \mid a_1$ or $p \mid b_0$ $\times$

$\Rightarrow p \mid a_1$

... keep going ...

$p \mid a_0, \; p \mid a_1, \; \cdots \; p \mid a_r$

$\Rightarrow p \mid a_r b_s$

$\Rightarrow p \mid c_n$ $\times$

$\blacksquare$

Example: $x^{17} + 125x - 35x^4 + 20x^3 - 5x^2 + 100x + 15$

irreducible over $\mathbb{Q}$ with $p=5$

Moral: if f irreducible over $\mathbb{C}$, then $\deg(f) \leq 1$

if f irreducible over $\mathbb{R}$, then $\deg(g) \leq 2$

Whereas over $\mathbb{Q}$ $\exists$ polynomials of arbitrarily large degree that are irreducible

The reduction test

About reducing coefficients modulo a prime

Let $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$ with $+, \times$ mod p (prime) be the field with p elements and

$$\sigma_p : \mathbb{Z} \longrightarrow \mathbb{F}_p \, ;$$

$$\sigma_p(a) = a \bmod p$$

Extend this to

$$\sigma_p^* : \mathbb{Z}_p[x] \longrightarrow \mathbb{F}_p[x]$$

$$\sigma_p^*\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \sigma_p(a_i) x^i$$

Example: $p=5$

$f = 8x^3 - 6x - 1 \in \mathbb{Z}[x]$

$\sigma_5^*(f) = 3x^2 + 4x + 4 \in \mathbb{F}_5[x]$

Theorem Reduction test

$f \in \mathbb{Z}[x]$ and p a prime s.t

(i) $\deg \sigma_p^*(f) = \deg(f)$

(ii) $\sigma_p^*(f)$ irreducible over $\mathbb{F}_p$

Then f irreducible over $\mathbb{Q}$

Example: $f = 8x^3 - 6x - 1$

$(p=2)$: $\sigma_2^*(f) = 1$ fails (i)

$(p=3)$: $\sigma_3^*(f) = 2x^3 + 2 \in \mathbb{F}_3[x]$ has root in $\mathbb{F}_3$

$(p=5)$: $\sigma_5^*(f) = 3x^3 + 4x + 4 \in \mathbb{F}_5[x]$ as $\deg \leq 3$, suffices to check has no roots in $\mathbb{F}_5 = \{0,1,2,3,4\}$

has none $\Longrightarrow$ irred over $\mathbb{F}_5$

$\Longrightarrow 8x^3 - 6x - 1$ irred over $\mathbb{Q}$

2. Fields and Extensions

Alternative definition of fields

Definition Field

A field is a set F with 2 binary operations, $+$ and $\times$ such that for any $a,b,c \in F$

1) F is an Abelian group under $+$;
2) $F \setminus \{0\}$ is an Abelian group under $\times$
3) The two operations are linked by the distributive law

Definition Field

A field is a set F with 2 binary operations, $+$ and $\times$ such that for any $a,b,c \in F$

1) F is a commutative ring under $+$ and $\times$;
2) $\forall\, a \in F \setminus \{0\}$, $\exists$ an $a^{-1} \in F$ with $a \times a^{-1} = 1 = a^{-1} \times a$

Field Extensions

Definition Extension

Let $F \subseteq E$ be fields

Then F is a subfield of E

E is an extension of F

If $\beta \in E$, then write $F(\beta)$ for the smallest subfield of E that contains F and β so in particular $F(\beta)$ is an extension of F.

In general, if $\beta_1, \dots, \beta_k \in E$, define $F(\beta_1, \dots, \beta_k) = F(\beta_1, \dots, \beta_{k-1})(\beta_k)$

Note: $F \subseteq F(\beta)$ is an extension

Say $F(\beta)$ is the result of adjoining β to F

Similarly $F(\beta_1, \beta_2, \dots, \beta_k)$

If $E = F(\beta)$ for some β then E is a simple extension

Example: $\mathbb{Q} \subseteq \mathbb{R}$, $\mathbb{Q} \subseteq \mathbb{C}$, $\mathbb{R} \subseteq \mathbb{C}$

$\mathbb{R} \subseteq \mathbb{R}(i)$

(notice: $\mathbb{R}(i) \subseteq \mathbb{C}$; on the otherhand,

$$a, b \in \mathbb{R} \underset{\mathbb{R}(i) \text{ field}}{\Longrightarrow} a + bi \in \mathbb{R}(i)$$

$$\Longrightarrow \mathbb{R}(i) = \mathbb{C})$$

Example: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ a simple extension

Firstly $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ and $b \in \mathbb{Q}(\sqrt{2})$ for any $b \in \mathbb{Q} \Rightarrow b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ fields closed under $\times$

Similarly $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ fields closed under $+$

Thus the set

$$\mathbb{F} = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subseteq \mathbb{Q}(\sqrt{2})$$

$\mathbb{F}$ is a field in its own right using the usual addition and multiplication of complex numbers

For example, inverse of $a + b\sqrt{2}$ is given by

$$\frac{1}{a + b\sqrt{2}} \times \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}$$

We have $\mathbb{Q} \subseteq \mathbb{F}$ and $\sqrt{2} \in \mathbb{F}$. Since $\mathbb{Q}(\sqrt{2})$ is the smallest field having this property $\Rightarrow \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{F}$.

Hence

$$\boxed{\mathbb{Q}(\sqrt{2}) = \mathbb{F} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}}$$

Example: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is also a simple extension

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

proof:

$$\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \Rightarrow \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$\Rightarrow \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

On the otherhand

$$(\sqrt{2} + \sqrt{3})^3 = (\sqrt{2})^3 + 3(\sqrt{2})^2(\sqrt{3}) + 3(\sqrt{2})(\sqrt{3})^2$$

$$= 2\sqrt{2} + 6\sqrt{3} + 9\sqrt{2} + 3\sqrt{3}$$

$$= 11\sqrt{2} + 9\sqrt{3}$$

Since $(\sqrt{2}+\sqrt{3})^3 \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ we get

$$(11\sqrt{2}+9\sqrt{3}) - 9(\sqrt{2}+\sqrt{3}) \in \mathbb{Q}(\sqrt{2}+\sqrt{3}) \Rightarrow 2\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

$$\Rightarrow \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$ since $1/2 \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, $\frac{1}{2}(2\sqrt{2})$

Similarly $\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$

$$\Longrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

Algebraic elements

Definition Algebraic

Let $F \subseteq E$ be an extension of fields and $\alpha \in E$

$\alpha \in E$ is algebraic over F when:

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

for some $a_0, a_1, \ldots, a_N \in F$. In otherwords α is a root of some $f \in F[x]$

Definition Trancendental

If α is not the root of any polynomial $f \in F[x]$ with F-coefficients then we say F is trancendental over F

Example:

- $\sqrt{2}$ algebraic over $\mathbb{Q}$ (roots of x^2-2)
- π NOT algebraic over $\mathbb{Q}$ $\longleftarrow$ transcendental
- π is algebraic over $\mathbb{Q}(\pi)$ (roots of $x-\pi$)
- The roots of x^2+4x+2 are algebraic over $\mathbb{Q}$

3. Quotients

Definition of Ideals

Definition Ideals of a ring

Let R be any ring and $I \subseteq R$ be any subset

The subset I is an **ideal** if

i) $0 \in I$

ii) $a \in I \implies -a \in I$

iii) $a, b \in I \implies a+b \in I$

iv) $a \in I, r \in R \implies ar, ra \in I$

Principal Ideal

Definition Principal ideal

The ideal

$$aR = \{ar : r \in R\}$$

is called **principal ideal** (generated element $a \in R$)

Principal Ideal Domain

Definition Principal Ideal Domain

A **principal ideal domain** (PID) is an integral domain (ID) where every ideal is principal

Theorem

Let F be any field. Then the ring

$$F[x]$$

is a principal ideal domain

Definition Ideal in polynomial rings over fields

An ideal in $F[x]$ is a set of the form

$$\langle f \rangle = \{ fg \mid g \in F[x] \}$$

for some fixed polynomial f

Example: $x^2-2 \in \mathbb{Q}[x]$ and ideal

$$\langle x^2-2\rangle = \{p(x^2-2) : p \in \mathbb{Q}[x]\}$$

Simplifying $x^3-2x+15+\langle x^2-2\rangle$;

$x^3-2x+15$ divisible by x^2-2

$$x^3-2x+15 = x(x^2-2)+15 \implies x^3-2x+15+\langle x^2-2\rangle = x(x^2-2)+15+\langle x^2-2\rangle$$

$$= 15+\langle x^2-2\rangle$$

Example: $\mathbb{F}_2[x]$ and ideal $\langle x\rangle$

There are only 2 cosets

$$0+\langle x\rangle \quad \text{and} \quad 1+\langle x\rangle$$

Suppose we have $g+\langle x\rangle$ and

- g has no constant term (namely 0 since $\mathbb{F}_2=\{0,1\}$)

$$g+\langle x\rangle = 0+\langle x\rangle = \langle x\rangle$$

$(\subseteq)$: $f \in g+\langle x\rangle \implies f = g+px$

no constant term

$\implies f$ has no constant term

$\implies f \in \langle x\rangle$

$(\supseteq)$: $f \in \langle x\rangle \implies f-g \in \langle x\rangle$

$$f = g+(f-g) \in g+\langle x\rangle$$

- g has a constant term

$$g+\langle x\rangle = 1+\langle x\rangle$$

Reminder of Cosets

Let $(G,+)$ be any Abelian group, $H \leq G$ subgroup

Definition Coset

$(G,+)$ be any Abelian group, $H \leq G$ subgroup. Then

$$\forall a \in G, \quad a+H = \{a+x \mid x \in H\} \leq G$$

is a coset of a relative to H.

In

$$\underset{\text{representative}}{a} + H$$

Properties of Cosets

Lemma

(i) $a+H = b+H \iff a-b \in H$

(ii) $a+H = b+H \iff (a+H) \cap (b+H) \neq \emptyset$

(iii) $a+H = H = 0+H \iff a \in H$

Proposition

$H \leq G$ and $(G,+)$ Abelian $\implies H \trianglelefteq G$ normal

Proof:

$$\forall h \in H, \quad h = hgg^{-1} = ghg^{-1} \quad \forall g \in G$$

$\blacksquare$

Factor Group

Definition Factor Group

Let $(G,+)$ be any Abelian group, $H \leq G$ subgroup.

$$G/H = \{a+H : a \in G\} = \{\text{set of all cosets in } G \text{ relative to } H\}$$

Factor/Quotient group

Factor Rings

Now let R be any ring $\implies (R,+)$ is an Abelian group.

Let $I \leq R$ be any ideal of R. Then

$I \leq R$ is a subgroup relative to $+ \implies$ we have R/I

Consider **factor set** R/I with binary operation

- Addition: $(a+I)+(b+I) = (a+b)+I$
- Multiplication: $(a+I)\times(b+I) = (a\times b)+I$

Proposition

The binary operations $+, \times$

$$+: (a+I)+(b+I) = (a+b)+I$$

$$\times: (a+I)\times(b+I) = (a\times b)+I$$

are **well-defined**

Definition Polynomial ring cosets

$\langle f \rangle \leq F[x]$ be an ideal and $g \in F[x]$ any polynomial. The set

$$g+\langle f \rangle = \{g+h \mid h \in \langle f \rangle\}$$

is called the **coset** of $\langle f \rangle$ with representative g

Proposition

$(R/I, +, \times)$ is a ring with $+, \times$ defined above

Fundamental Theorem of Homomorphisms for Rings

Theorem

Let R, S be any rings and $\alpha: R \longrightarrow S$ be a homomorphism

Then $\ker\alpha \leq R$ an ideal of R and $\operatorname{Im}\alpha \leq S$ is a subring of S and

$$R/\ker\alpha \cong \operatorname{Im}\alpha$$

4. Field Contruction

Proper Ideals

Definition Proper Ideals

Let R be any ring

An ideal of R is proper if $I \neq R$

Maximal Ideals

Definition Maximal Ideals

An ideal M of R is maximal if

(i) M is proper, $M \neq R$

(ii) For any ideal $I \subseteq R$

$$M \subseteq I \subseteq R \implies I = M \text{ or } I = R$$

Properties of Maximal Ideals

Theorem

Let R be any commutative ring with $1 \in R$. Let M be any ideal of R. Then

$$M \text{ maximal} \iff R/M \text{ is a field}$$

Now consider $R = F[x]$, F a field and f irreducible over F

Let $\langle f \rangle \subseteq I \subseteq F[x]$ for an ideal I. Then

$$I = \langle h \rangle \implies \langle f \rangle \subseteq \langle h \rangle$$

$$\implies h \mid f$$

Since f irreducible $\implies$ h constant $c \in F$ or $h = cf$

$$\implies I = \langle c \rangle \text{ or } I = \langle cf \rangle$$

But $\langle cf \rangle = \langle f \rangle$

On the otherhand, any polynomial g can be written as a multiple of c by setting

$$g = c(c^{-1}g) \implies \langle c \rangle = F[x]$$

Thus if f is an irreducible polynomial $\Rightarrow \langle f \rangle$ is maximal

Conversely if $\langle f \rangle$ is maximal and $h|f \Rightarrow \langle f \rangle \subseteq \langle h \rangle$ so that by maximality

$$\langle h \rangle = \langle f \rangle \text{ or } \langle h \rangle = F[x]$$

Note that $\langle f \rangle = \langle h \rangle \Leftrightarrow h = cf$ for some constant $c \in F$ (prove!)

Similarly if $h = F[x] \Leftrightarrow h = c$ some constant (prove!)

Hence f irreducible over F. Thus

$$\boxed{\text{ideal } \langle f \rangle \text{ is maximal} \Leftrightarrow f \text{ irreducible}}$$

Corollary

$F[x]/\langle f \rangle$ is a field $\Leftrightarrow f$ is an irreducible polynomial over F

Example: x^2+1 irreducible over $\mathbb{R} \Rightarrow \mathbb{R}/\langle x^2+1 \rangle$ a field.

Constructing fields

Example: a field of order 4

idea: $f \in F[x]$ irreducible over F

$$\Rightarrow F \subseteq F[x]/\langle f \rangle \leftarrow \text{new field}$$

Start with $\mathbb{F}_2 = \{0,1\}$ $+, \times \bmod 2$ and

$x^2+x+1 \in \mathbb{F}_2[x]$ irreducible over $\mathbb{F}_2$ $\quad 0^2+0+1=1$

$\Rightarrow \mathbb{F}_2[x]/\langle x^2+x+1 \rangle$ is a field $\quad 1^2+1+1=1$ $\quad$ no roots

with elements: $\{g+\langle x^2+x+1 \rangle : g \in \mathbb{F}_2[x]\}$ where

$$\begin{aligned} g+\langle x^2+x+1 \rangle &= q(x^2+x+1)+r+\langle x^2+x+1 \rangle \\ &= r+\langle x^2+x+1 \rangle \\ &= (ax+b)+\langle x^2+x+1 \rangle \quad \text{— } (*) \end{aligned}$$

Notation: $(a=1, b=0)$ $x+\langle x^2+x+1 \rangle \stackrel{def}{=} \alpha$

Also $(a=0)$ $b+\langle x^2+x+1 \rangle$ is written as $b \in \mathbb{F}_2$

Then

$$(*) = (a+\langle x^2+x+1\rangle)(x+\langle x^2+x+1\rangle) + (b+\langle x^2+x+1\rangle)$$

$$= a\alpha + b$$

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ so that e.g

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

$$= \alpha^2+1$$

Magic algebraic rule: $qf + \langle f\rangle = \langle f\rangle$

$$(x^2+x+1) + \langle x^2+x+1\rangle = \langle x^2+x+1\rangle$$

$\implies \alpha^2+\alpha+1 = 0$

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

Carrying on: $\alpha^2+1 = \alpha+1+1 = \alpha$

Drawing table

$\mathbb{F}_4$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

General construction of fields: field with p^d elements, p prime, $d \geq 1$

Start with $\mathbb{F}_p[x]$ and $f \in \mathbb{F}_p[x]$ irreducible of degree d.

Let $\alpha = x + \langle f\rangle$ and replace $\mathbb{F}_p$ with its isomorphic copy in $\mathbb{F}_p[x]/\langle f\rangle$.

This gives

$$\mathbb{F}_p[x]/\langle f\rangle = \{a_{d-1}\alpha^{d-1} + \cdots + a_0 \mid a_i \in \mathbb{F}_p\}$$

Example: Field with 81 elements

$$= 9^2 = 3^4 = (3^2)^2$$

Step 1: Construct $\mathbb{F}_{3^2} = \mathbb{F}_9$

$$f = x^2+1 \quad \left.\begin{array}{l} 0^2+1=1 \\ 1^2+1=2 \\ 2^2+1=2 \end{array}\right\} \begin{array}{c}\text{no roots} \\ + \\ \text{quadratic}\end{array} \Longrightarrow \text{irred over } \mathbb{F}_3$$

$\Longrightarrow \mathbb{F}_9 = \{a+b\alpha : a,b \in \mathbb{F}_3\}$ with rule $\alpha^2+1=0 \Longrightarrow \alpha^2=2$

$= \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$

Step 2: Construct $\mathbb{F}_{9^2} = \mathbb{F}_{81}$

$\mathbb{F}_9[y] \ni g = y^2+y+\alpha$

Check has no roots in $\mathbb{F}_9$:

$$g(\alpha+1) = (\alpha+1)^2 + (\alpha+1) + \alpha$$
$$= \alpha+1$$

Similarly for other 8

$\mathbb{F}_{81} = \{A + B\beta : A, B \in \mathbb{F}_9\}$ and $\beta^2+\beta+\alpha=0 \Longrightarrow \beta^2 = 2\beta+2\alpha$

$= \{a+b\alpha+c\beta+d\alpha\beta : a,b,c,d \in \mathbb{F}_3\}$ and $\alpha^2=2$, $\beta^2 = 2\beta+2\alpha$

Example: Field of order 729

$729 = 3^6 = (3^2)^3$

1) Consider the polynomial

$$f = x^2+x+2 \in \mathbb{F}_3[x]$$

Has no roots:
$$\left.\begin{array}{l} \blacktriangleright\ 0^2+0+2=2 \\ \blacktriangleright\ 1^2+1+2=1 \\ \blacktriangleright\ 2^2+2+2=2 \end{array}\right\} \Rightarrow f \text{ is irreducible}$$

$\Rightarrow \mathbb{F}_9 = \mathbb{F}_3[x]/\langle x^2+x+2\rangle.$

Let $\alpha = x + \langle x^2+x+2\rangle \Longrightarrow \mathbb{F}_9 = \{a\alpha+b : a,b \in \mathbb{F}_3\}$ with rule $\alpha^2 = 2\alpha+1$

Now let X be a new variable and consider the polynomials $\mathbb{F}_q[X]$ over $\mathbb{F}_q$.

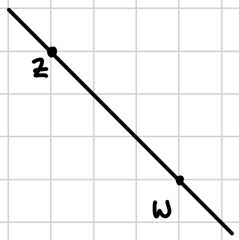
In this new variable, consider polynomial

$$g = X^3 + (2\alpha+1)X + 1$$

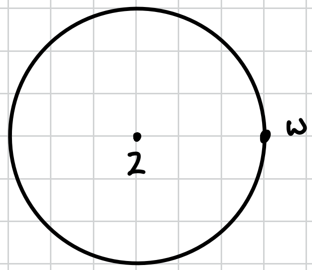
5. Constructibility

Constructing in $\mathbb{C}$

There are 2 constructions in $\mathbb{C}$. For $z, w \in \mathbb{C}$



line through z, w



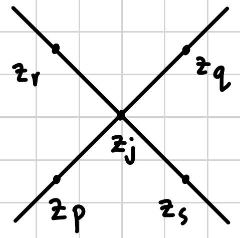
circle centered at z passing through w

Definition Constructible

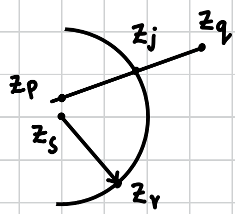
A $z \in \mathbb{C}$ constructible $\iff \exists$ a sequence

$$0, 1, 2, z_1, z_2, \dots, z_k = z$$

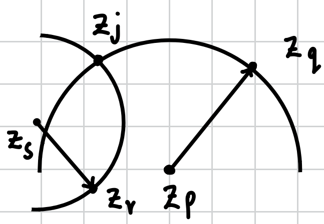
Each z_j obtained from earlier numbers in the sequence in one of the following 3 ways



(i)



(ii)



(iii)

with $p, q, r, s < j$

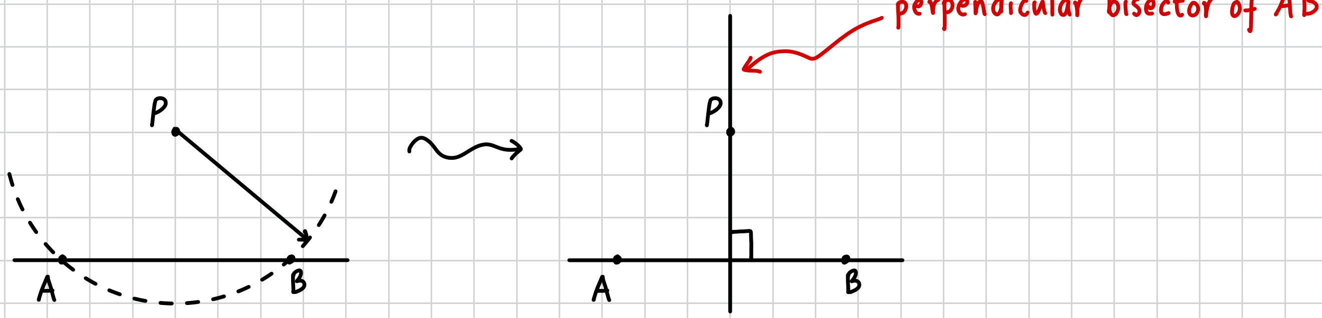
Given $0, 1, i$ for free so they are indisputably constructible. The reasoning is if you stand on a plane without co-ordinates, then your position can be taken as 0.

Declare a direction to be the real axis and a distance along it to be 1.

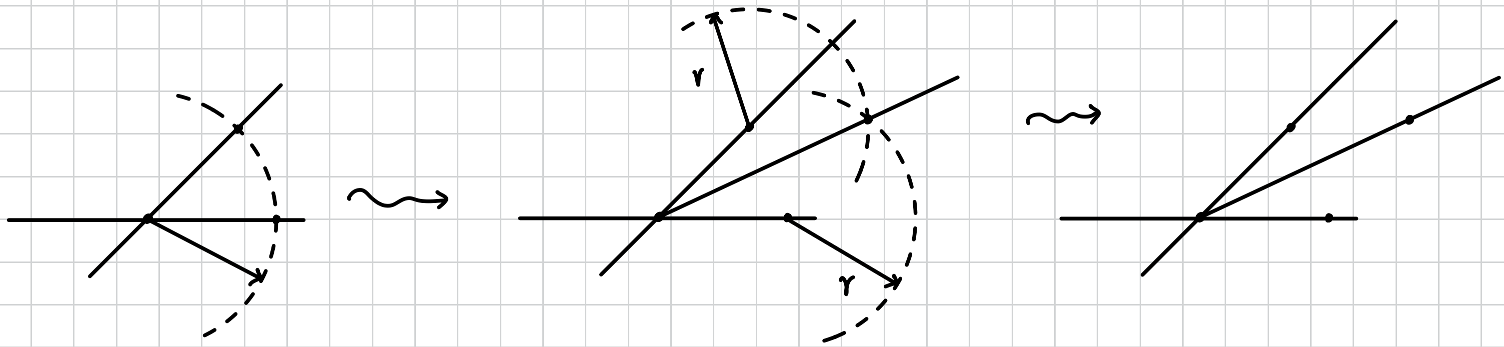
Construct a perpendicular bisector of segment -1 to 1 and then measure a unit distance along to get i

We have 4 other constructions

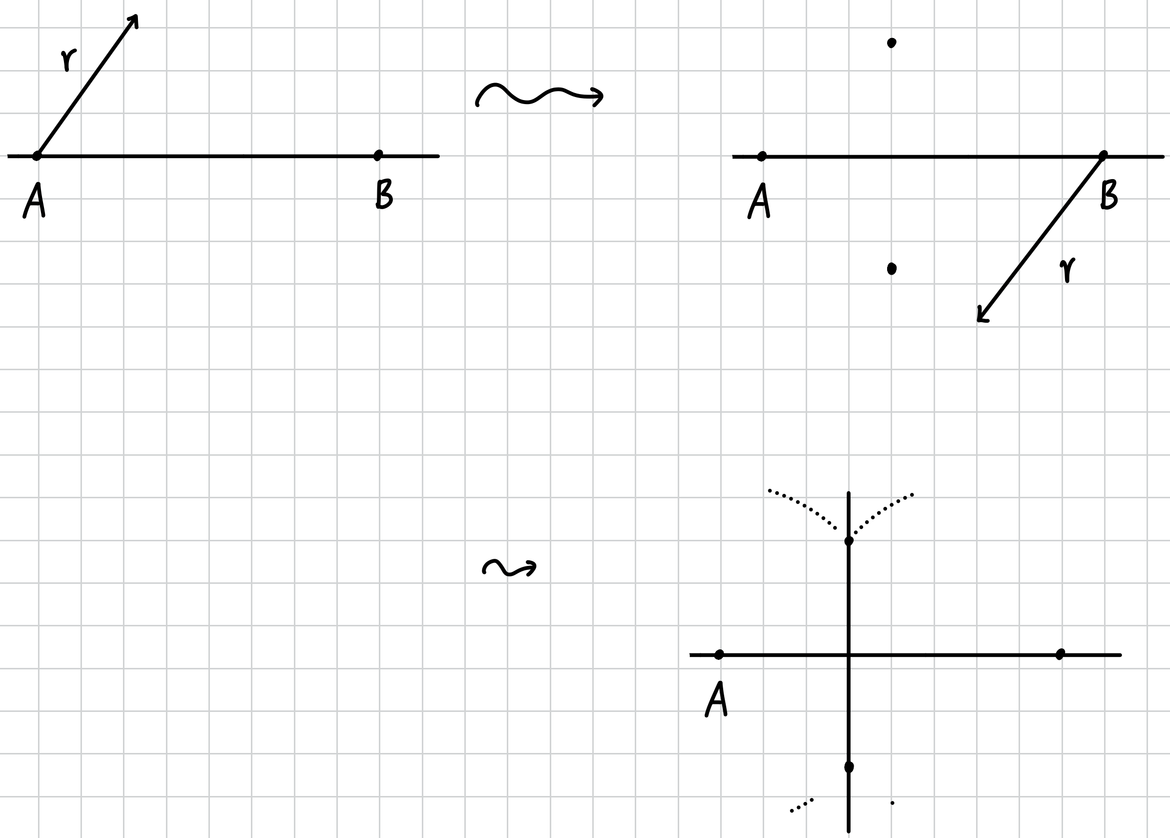
1) Dropping a perpendicular from a point to a line



2) bisect angles

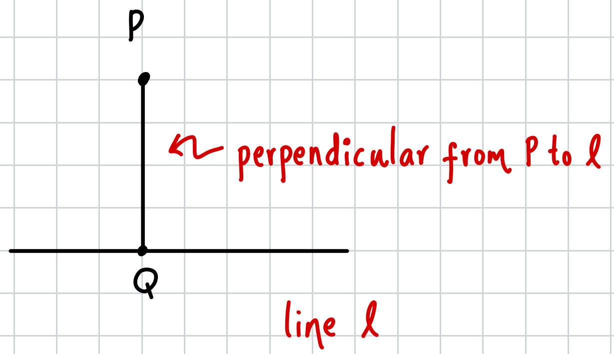


3) drawing a perpendicular bisector

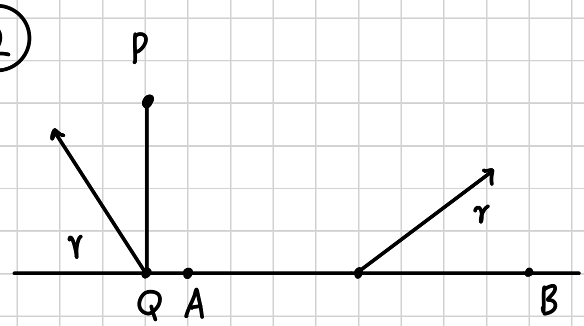


4) Draw a line through a point that is parallel to some other line.

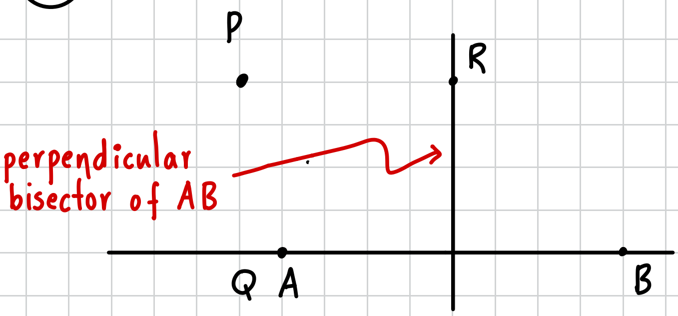
1



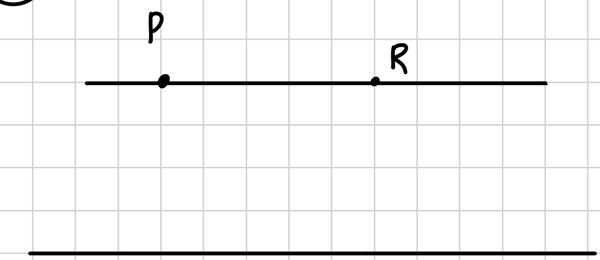
2



3



4

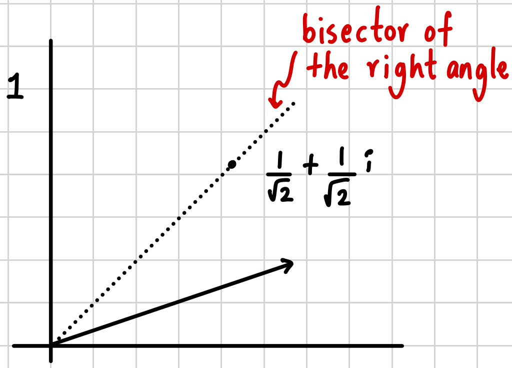


Notation

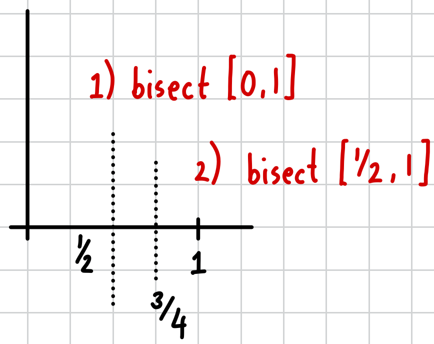
Write $\mathcal{C}$ for the set of constructible numbers.

Example: Constructing 3

Constructing $\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i$



Constructing $3/4$



Theorem

$\mathcal{C}$ is a subfield of $\mathbb{C}$

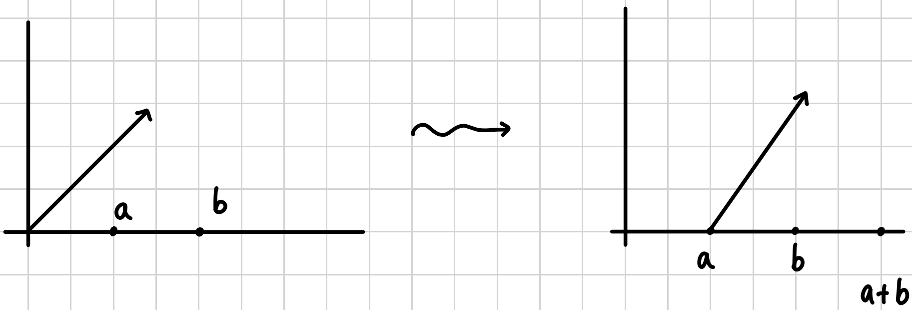
Proof:

Show first that $\mathcal{C} \cap \mathbb{R}$ are a subfield of $\mathbb{R}$, i.e.

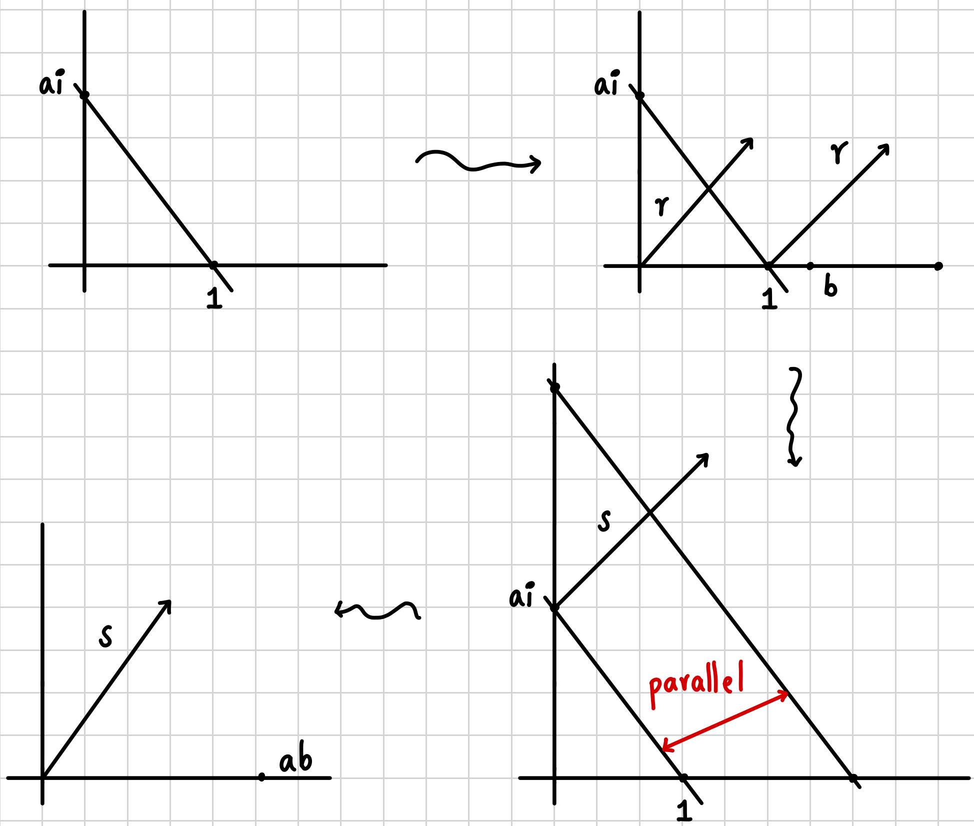
$$a, b \in \mathcal{C} \cap \mathbb{R} \Longrightarrow a+b,\ -a,\ ab \text{ and } a^{-1} = \frac{1}{a} \in \mathcal{C} \cap \mathbb{R}$$

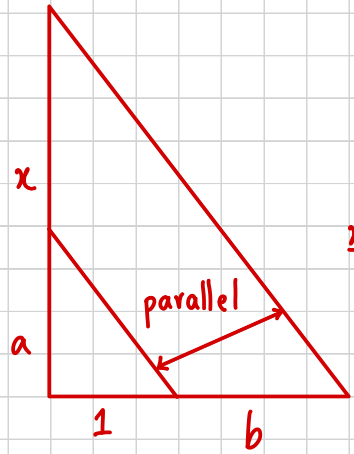
- Closed under $-$:

- Closed under $+$:



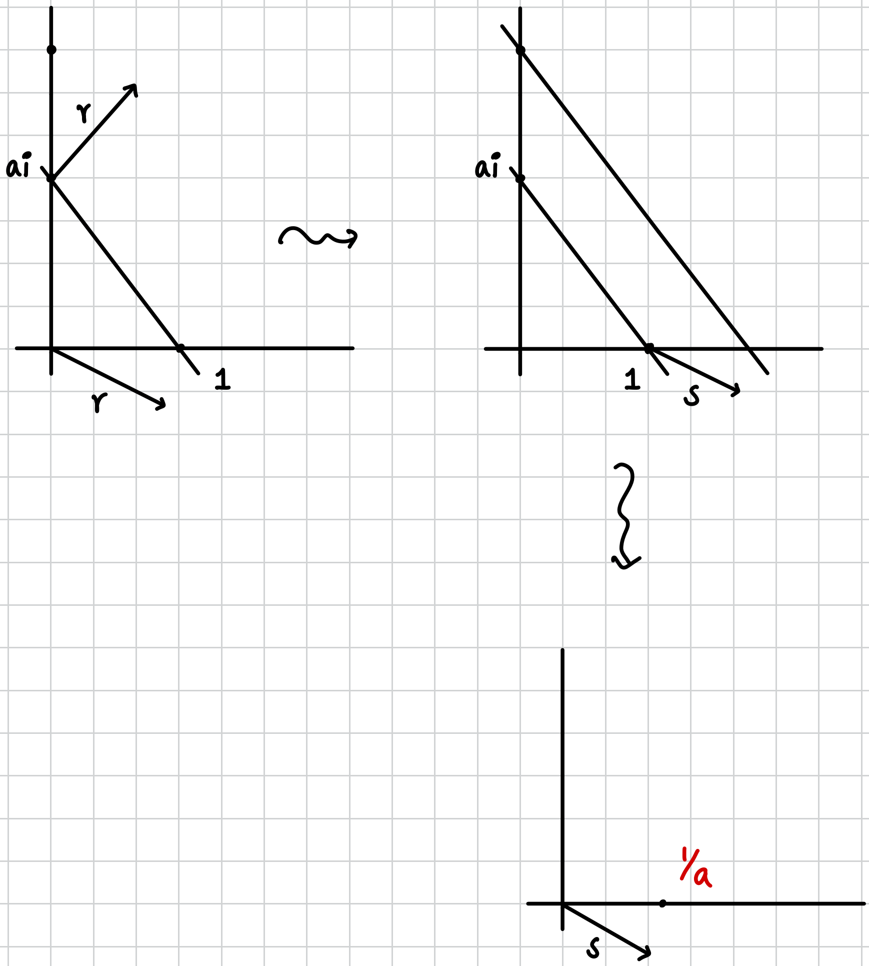
- Closed under $\times$:





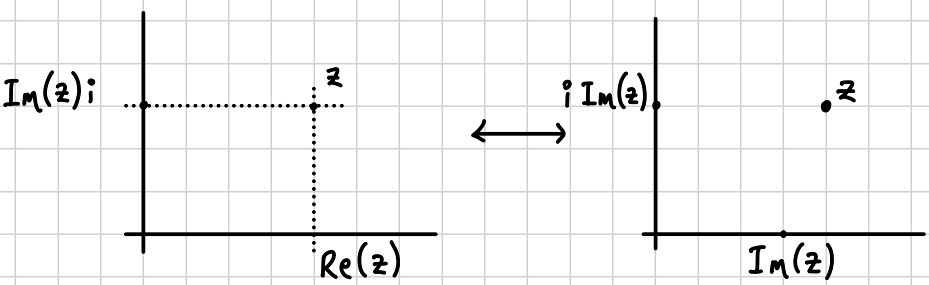
$$\frac{x+a}{a} = b+1 \implies x = ab$$

- <u>Closed under $\div$</u> :



Now showing $\mathcal{C}$ subfield of $\mathbb{C}$: $z+w$, $-z$, zw, $1/z$ are constructible

<u>First</u> : $z \in \mathbb{C}$ constructible $\iff$ $\mathrm{Re}(z)$ and $\mathrm{Im}(z)$ constructible



<u>Second</u>: if $z, w \in \mathbb{C}$ then

$$z+w = (\mathrm{Re}(z) + \mathrm{Re}(w)) + (\mathrm{Im}(z) + \mathrm{Im}(w))i$$

$$zw = (\mathrm{Re}(z)\mathrm{Re}(w) - \mathrm{Im}(z)\mathrm{Im}(w)) + (\mathrm{Re}(z)\mathrm{Im}(w) + \mathrm{Im}(z)\mathrm{Re}(w))i$$

$$\frac{1}{z} = \frac{\mathrm{Re}(z) - \mathrm{Im}(z)i}{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2}$$

So that for example if $z, w \in \mathcal{C}$

$\Rightarrow \mathrm{Re}(z), \mathrm{Re}(w), \mathrm{Im}(z), \mathrm{Im}(w) \in \mathcal{C} \cap \mathbb{R}$

$\Rightarrow \mathrm{Re}(z) + \mathrm{Re}(w), \mathrm{Im}(z) + \mathrm{Im}(w) \in \mathcal{C} \cap \mathbb{R}$

$\Rightarrow \mathrm{Re}(z+w), \mathrm{Im}(z+w) \in \mathcal{C} \cap \mathbb{R}$

$\Rightarrow z+w \in \mathcal{C}$

Similar for $zw, -z, \frac{1}{z} \in \mathcal{C}$ $\blacksquare$

6. Vector Spaces and Degrees

Definition of a Vector Space

Definition Vector Space

Let $\mathbb{F}$ be a field (usually $\mathbb{R}$ or $\mathbb{C}$). A vector space over $\mathbb{F}$ is a set V together with binary operations

vector addition

$$V \times V \longrightarrow V$$
$$(u,v) \longmapsto (u+v)$$

scalar multiplication

$$\mathbb{F} \times V \longrightarrow V$$
$$(\alpha, v) \longmapsto \alpha v$$

(A1) commutativity over addition

$$u+v = v+u \quad \forall u,v \in V$$

(A2) associativity over addition

$$u+(v+w) = (u+v)+w \quad \forall u,v,w \in V$$

(A3) $\underline{0}$ vector

$$\exists\, \underline{0} \in V \text{ such that } \underline{0}+v = v \quad \forall v \in V$$

(A4) Inverse

Given any $v \in V$, $\exists\, -v \in V$ with $(-v)+v = \underline{0}$

(M1) Distributivity

$$\alpha(u+v) = \alpha u + \beta v \quad \forall \alpha \in \mathbb{F},\ u,v \in V$$

(M2) Scalar Multiplication

$$\alpha(\beta v) = (\alpha\beta)v \quad \forall \alpha, \beta \in \mathbb{F} \text{ and } v \in V$$

(M3) Distributivity

$$(\alpha+\beta)v = \alpha v + \beta v \quad \forall \alpha, \beta \in \mathbb{F},\ v \in V$$

(M4) Multiplicative Identity

$$1v = v \quad \forall v \in V \qquad (\text{where } 1 \in \mathbb{F} \text{ is the usual } 1)$$

- A vector is an element of a vector space
- Given a vector space V over a field $\mathbb{F}$, any $\alpha \in \mathbb{F}$ is a scalar

Note

i) Being binary operation implies V is closed under linear combination

$\forall u, v \in \mathbb{F}$ and any $\alpha \in \mathbb{F}$, $u+v \in V$, $\alpha v \in V$

ii) Axioms A1 - A4 together with binary operation addition is an abelian group

Linear Combination

Definition Linear Combination

Given vectors $\underline{v}_1, \dots, \underline{v}_q \in V$ and scalars $\alpha_1, \dots, \alpha_q \in \mathbb{F}$, the sum

$$\alpha_1 \underline{v}_1 + \dots + \alpha_q \underline{v}_q = \sum_{j=1}^{q} \alpha_j \underline{v}_j$$

is called the linear combination

Linear Dependance/Independence

Definition Linear dependence

A collection of vectors $\mathcal{C} = \{\underline{v}_1, \dots, \underline{v}_q\} \subseteq V$ is linearly dependant if $\exists (\alpha_1, \dots, \alpha_q) \in \mathbb{F}^q \setminus \{(0, \dots, 0)\}$ s.t

$$\alpha_1 \underline{v}_1 + \dots + \alpha_q \underline{v}_q = \underline{0}$$

Otherwise, we say $\underline{v}_1, \dots, v_q$ are linearly independant

Definition Linear independence

$\underline{v}_1, \dots, \underline{v}_q$ are linearly independent if

$$\alpha_1 \underline{v}_1 + \dots + \alpha_q \underline{v}_q = \underline{0} \implies \alpha_1 = 0, \dots, \alpha_q = 0$$

Spans

Definition Span

Let $\mathcal{C} \subset V$ be a non-empty collection of vectors.

The span of $\mathcal{C}$ denoted

$$Sp(\mathcal{C})$$

is the set of all linear combination of $\mathcal{C}$

$$Sp(\mathcal{C}) = \{ \underline{u} \in \mathbb{F}^n \mid \underline{u} = \alpha_1 \underline{v}_1 + \cdots + \alpha_n \underline{v}_n \text{ for some } \alpha_i \in \mathbb{F},\ \underline{v}_i \in S \}$$

By convention, $\boxed{Sp(\emptyset) = \{\underline{0}\}}$

Basis

Definition Basis

Let $S \subseteq V$ be a non-trivial $S \neq \{0\}$ subspace of V,

A collection $B = \{\underline{v}_1, \cdots, \underline{v}_q\} \subseteq S$ forms a basis if

i) $\underline{v}_1, \cdots, \underline{v}_q$ is linearly independent

ii) $sp(\underline{v}_1, \cdots, \underline{v}_q) = S$

By definition,

$\boxed{\text{basis of } \{0\} \text{ is } \emptyset}$

Dimensions

Definition Dimensions

For any subspace $S \subseteq V$, we define dimension of S by

$$\dim(S) = \#(\text{basis of } S) \quad \text{cardinality}$$

Vector Space homomorphism

Vector space homomorphism is a linear map

Definition Linear Maps

Let V, W be vector spaces over the same field $\mathbb{F}$.

A map $L: V \longrightarrow W$ is called linear map if

$$L(\alpha \underline{u} + \beta \underline{v}) = \alpha L(\underline{u}) + \beta L(\underline{v}) \qquad \forall \alpha, \beta \in \mathbb{F}, \ \forall \underline{u}, \underline{v} \in V$$

In abstract algebra, linear maps are referred to as vector space homomorphism, since they like other homomorphisms, they are structure-preserving maps.

Therefore we denote the set of all linear maps from V to W by

$$\mathrm{Hom}(V, W)$$

Example: $V = \mathbb{C}$ is a vector space over $F = \mathbb{R}$

"vectors": $a + bi \in \mathbb{C}$ $\qquad \begin{pmatrix} a \\ b \end{pmatrix}$

"scalars" $c \in \mathbb{R}$
$\in F$

" vector +": $(a+bi) + (c+di)$ $\qquad \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix}$

"scalar x": $c(a+bi)$ $\qquad c\begin{pmatrix} a \\ b \end{pmatrix}$

basis: $\{1, i\}$ $\qquad \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$\Longrightarrow$ $\mathbb{C}$ a 2-dimensional vector space over $\mathbb{R}$

Example: let $F \subseteq E$ be an extension of fields

Then E is a vector space over F

"vectors": elements of E

"scalars": elements of F

"vectors +": $+$ in E

"scalar multiplication": product of an element of F with an element of E inside E

Degree of an extension

Definition Degree

Let $F \subseteq E$ be an extension of fields

Consider E as a vector space over F and define **degree** of the extension to be the dimension of this vector space denoted

$$[E:F]$$

Call $F \subseteq E$ a finite extension if the degree is finite

Recall: F a field

$F[x]$ = polynomials with F-coefficients

$f \in F[x]$

ideal: $\langle f \rangle = \{ fh : h \in F[x] \}$

coset: $g + \langle f \rangle = \{ g + fh : h \in F[x] \}$

Properties:

(i) $g + \langle f \rangle = \langle f \rangle \iff g \in \langle f \rangle$

(ii) $gf + \langle f \rangle = \langle f \rangle$

$$\boxed{\begin{aligned} F[x]/\langle f \rangle &= \{ \text{all cosets of } \langle f \rangle \} \\ &= \{ g + \langle f \rangle : g \in F[x] \} \end{aligned}}$$

- Addition: $(g_1 + \langle f \rangle) + (g_2 + \langle f \rangle) = (g_1 + g_2) + \langle f \rangle$
- Multiplication: $(g_1 + \langle f \rangle)(g_2 + \langle f \rangle) = (g_1 g_2 + \langle f \rangle)$

$$\boxed{F[x]/\langle f \rangle \text{ is a field} \iff f \text{ is an irreducible polynomial over } F}$$

Finally, the cosets

$$a+\langle f\rangle$$

where $a\in F$ (i.e. $g+\langle f\rangle$ with g a constant polynomial).

Then $\{a+\langle f\rangle : a\in F\}$ is a "copy" of the original field F sitting inside $F[x]/\langle f\rangle$

(by copy, we mean isomorphic)

$$(a+\langle f\rangle)(b+\langle f\rangle) = ab+\langle f\rangle$$

$$(a+\langle f\rangle)+(b+\langle f\rangle) = (a+b)+\langle f\rangle$$

i.e. have (writing F as well as this other version of F)

$$F\subseteq F[x]/\langle f\rangle$$

an extension of fields when f irreducible over F

Theorem

If f is irreducible over F then the extension

$$F\subseteq F[x]/\langle f\rangle$$

has degree equal to degree of f

Proof:

Replace F by its isomorphic copy $\{a+\langle f\rangle : a+\langle f\rangle\}$

Claim: $B=\{1+\langle f\rangle, x+\langle f\rangle, \ldots, x^{d-1}+\langle f\rangle\}$ where $d=\deg(f)$ a basis

Span: $g+\langle f\rangle = (\underbrace{qf}_{\in} + r)+\langle f\rangle$ $\deg r<\deg f$

$$= r+\langle f\rangle$$

$$= (a_0+a_1x+\cdots+a_{d-1}x^{d-1})+\langle f\rangle$$

$$= (a_0+\langle f\rangle)(1+\langle f\rangle)+(a_1+\langle f\rangle)(x+\langle f\rangle)+\cdots+(a_{d-1}+\langle f\rangle)(x^{d-1}+\langle f\rangle)$$

an F-linear combination of B

Linear independence:

$$(a_0+\langle f\rangle)(1+\langle f\rangle)+\cdots+(a_{d-1}+\langle f\rangle)(x^{d-1}+\langle f\rangle) = 0+\langle f\rangle$$

$$\Rightarrow (a_0+a_1x+\cdots+a_{d-1}x^{d-1})+\langle f\rangle = \langle f\rangle$$

$\Rightarrow a_0 + \cdots + a_{d-1}x^{d-1} \in \langle f \rangle$

Everything in $\langle f \rangle$ has degree $\geq d$ except 0

$\Longrightarrow a_0 + \cdots + a_{d-1}x^{d-1} = 0$

$\Longrightarrow a_0 = 0,\ a_1 = 0,\ \cdots,\ a_{d-1} = 0$

$\Longrightarrow a_0 + \langle f \rangle, \dots, a_{d-1} + \langle f \rangle$ are 0 in $F[x]/\langle f \rangle$

$\blacksquare$

Simple extensions

Theorem Simple extensions

Let $F \subseteq E$ and $\alpha \in E$ algebraic over F. Then

(1) $\exists$ a unique $f \in F[x]$ that is monic, irreducible over F and has α as a root

(2) $F(\alpha) \cong F[x]/\langle f \rangle$

(3) $F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{d-1}\alpha^{d-1} \mid a_0, a_1, \dots, a_{d-1} \in F\}$ and $d = \deg(f)$.

In particular $B = \{1, \alpha^2, \dots, \alpha^{d-1}\}$ is a basis for $F(\alpha)$ over F

Definition Minimum Polynomial

The polynomial in (1) is called the minimum polynomial of α over F

Example: $F = \mathbb{Q}$, $\alpha = \sqrt[5]{2}$

Then $f = x^5 - 2 \in \mathbb{Q}[x]$

- monic
- α a root
- irreducible over $\mathbb{Q}$ Eisenstein

$\Longrightarrow f$ is the minimum polynomial of $\sqrt[5]{2}$ over $\mathbb{Q}$

$\Longrightarrow \mathbb{Q}(\sqrt[5]{2}) = \{a_0 + a_1\sqrt[5]{2} + a_2(\sqrt[2]{5})^2 + \cdots + a_4(\sqrt[2]{5})^4\}$, $[\mathbb{Q}(\sqrt[2]{5}) : \mathbb{Q}] = 5$

Example: $f = x^2 + 1 \in \mathbb{R}[x]$

Then f has a root $i \in \mathbb{C}$ is monic, irreducible over $\mathbb{R}$

$\Longrightarrow f$ minimal polynomial of α over $\mathbb{R}$

$\Longrightarrow \mathbb{R}(i) \cong \mathbb{R}[x]/\langle x^2 + 1 \rangle$

where $\mathbb{R}[x]/\langle x^2+1\rangle = \{g+\langle x^2+1\rangle : g\in\mathbb{R}[x]\}$ where $g+\langle x^2+1\rangle = q(x^2+1)+r+\langle x^2+1\rangle$

$$= r+\langle x^2+1\rangle$$

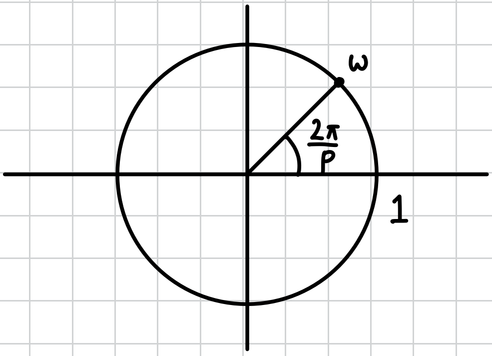
$$= (a+bx)+\langle x^2+1\rangle$$

e.g: $(x+\langle x^2+1\rangle)^2 = (x+\langle x^2+1\rangle)(x+\langle x^2+1\rangle)$

$$= x^2+\langle x^2+1\rangle$$

$$= 1(x^2+1)-1+\langle x^2+1\rangle = -1+\langle x^2+1\rangle$$

Example $\omega = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ (p prime)



$F=\mathbb{Q}$

guess #1 for min polynomial:

x^p-1
- monic ✓
- $\in\mathbb{Q}[x]$ ✓
- ω is a root ✓
- irreducible over $\mathbb{Q}$ ✗

But $x^p-1 = (x-1)(1+x+x^2+\cdots+x^{p-1})$

guess #2: $1+x+x^2+\cdots+x^{p-1}$
- $\in\mathbb{Q}[x]$
- monic
- ω a root
- irreducible prob sheet 4, Q2

(p th cyclotonic polynomial)

$\Longrightarrow [\mathbb{Q}(\omega):\mathbb{Q}] = p-1$

The Tower Law

Theorem The tower law

Consider a tower of extensions:

$$F\subseteq E\subseteq L$$

where E has finite degree over F and L has finite degree over E, then

$$[L:F]=[L:E][E:F]$$

(write proof later)

Example: What is the degree of:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, i)$$

i.e. $\underset{F}{\mathbb{Q}} \subseteq \underset{E}{\mathbb{Q}(\sqrt[3]{2})} \subseteq \underset{L}{\mathbb{Q}(\sqrt[3]{2}, i)}$

(i) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ is similar to the above with x^3-2 the min poly of $\sqrt[3]{2}$ over $\mathbb{Q}$

$$\Rightarrow [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

(and $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$ is a basis)

(ii) Now let $\mathbb{F} = \mathbb{Q}(\sqrt[3]{2})$, so that the second extension is

$$\mathbb{F} \subseteq \mathbb{F}(i)$$

and where the minimum polynomial of i over $\mathbb{F}$ is x^2+1

- monic
- i as a root
- irreducible over $\mathbb{F}$ as $i, -i \notin \mathbb{F}$

$\Rightarrow$ x^2+1 is the min poly

$[\mathbb{Q}(\sqrt[3]{2}, i), \mathbb{Q}(\sqrt[3]{2})] = 2$ basis $\{1, i\}$ for $\mathbb{F}(i)$ over $\mathbb{F}$

Tower law $\Rightarrow [\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}] = 3 \times 2 = 6$

proof $\Rightarrow$ $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, i, \sqrt[3]{2}\,i, (\sqrt[3]{2})^2 i\}$ a basis

(prove basis later)

7. Constructibility II

Theorem

A $z \in \mathbb{C}$ is constructible

$$\Updownarrow$$

$\exists$ a sequence of extensions:

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \qquad (*)$$

such that $\mathbb{Q}(z) = K_n$ ($\Leftrightarrow z \in K_n$) and K_i is an extension of K_{i-1} of degree ≤ 2

Corollary

$z \in \mathbb{C}$ constructible $\Longrightarrow$ degree of the extension $\mathbb{Q} \subseteq \mathbb{Q}(z)$ is a power of 2

Proof:

By theorem, $z \in K_n$ for the sequence $(*)$ hence

$$[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(z)][\mathbb{Q}(z) : \mathbb{Q}] \quad \text{by tower law}$$

where $[K_n : \mathbb{Q}] = \underbrace{[K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : \mathbb{Q}]}_{\text{all } 1 \text{ or } 2}$

$$= 2^m$$

Thus $[\mathbb{Q}(z) : \mathbb{Q}]$ divides 2^m

$$\Longrightarrow [\mathbb{Q}(z) : \mathbb{Q}] = 2^n \quad \text{for some } n$$

■

Moral: Tells us when $z \in \mathbb{C}$ cannot be constructed

Example Constructing regular n-gons

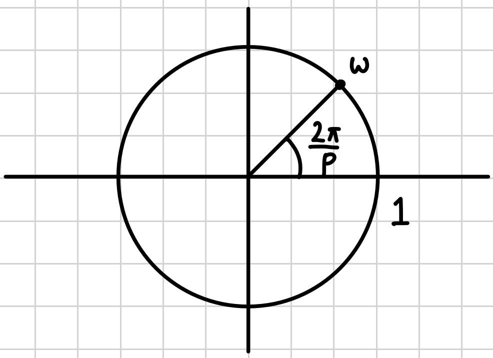
Exercise: an n-gon can be constructed iff

$$w = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \text{ can be constructed}$$

For $n = p$ prime, a p-gon constructible

$$\text{if } w = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p} \text{ constructible}$$

where $[\mathbb{Q}(w) : \mathbb{Q}] = p-1$



Thus for p-gon to be constructible

$$p-1 = 2^n \implies p = 2^n + 1$$

<u>Aside</u>:

m odd then

$$(x^m+1) = (x+1)(x^{m-1} - x^{m-2} + \cdots - x + 1)$$

so that if $n = mk$, m odd.

$$2^n + 1 = (2^k)^m + 1$$

$$= (2^k+1)((2^k)^{m-1} - \cdots - 2^k + 1) \quad \text{not prime}$$

Hence 2^n+1 to be prime, n can't have odd divisors $\implies n = 2^t$

i.e. if p-gon constructible

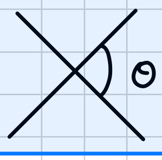
$$p = 2^{2^t} + 1$$

$\delta \in \mathbb{C}$ constructible $\implies [\mathbb{Q}(\delta) : \mathbb{Q}] = p^n$

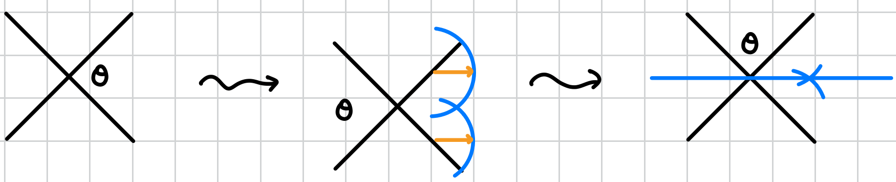
find minimal polynomial of deg $= 2^k$

Definition

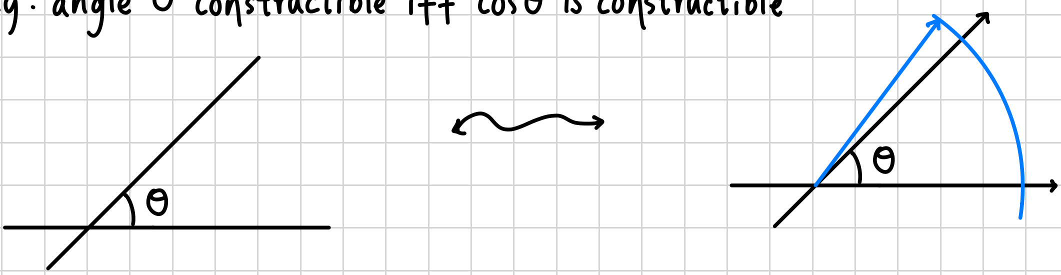
An angle θ is constructible iff you can construct



We know angles can always be bisected

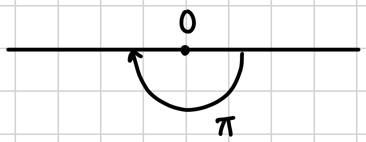


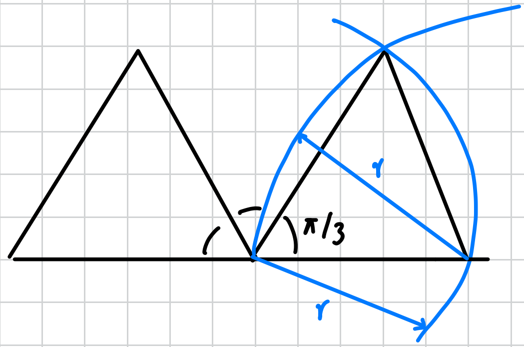
Finally: angle θ constructible iff $\cos\theta$ is constructible



Can angles always be trisected ?

Eg: yes for $\theta = \pi$





But $\theta = \frac{\pi}{3}$ cannot be trisected $\iff$ $\frac{\pi}{9}$ cannot be constructed

Exercise: $\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$ (compute $(\cos\varphi + i\sin\varphi)^3$ and De Moivre's Thm) $(*)$

Show $\cos\frac{\pi}{9}$ cannot be constructed by computing the degree of extension $\mathbb{Q} \subseteq \mathbb{Q}(\cos \pi/9)$

Have by $(*)$ that

$$\underbrace{\cos\frac{\pi}{3}}_{1/2} = 4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9} \implies 1 = 8\cos^3\frac{\pi}{9} - 6\cos\frac{\pi}{9}$$

Let $u = 2\cos\frac{\pi}{9}$ so that

$$u^3 - 3u - 1 = 0$$

- $2\cos\frac{\pi}{9}$ a root
- monic
- $\in \mathbb{Q}[x]$

Applying reduction test with $p=2 \implies$ irreducible

$\implies$ thus $u^3 - 3u - 1$ is the min polynomial of $2\cos\left(\frac{\pi}{3}\right)$ over $\mathbb{Q}$

$$\implies [\underbrace{\mathbb{Q}(2\cos\tfrac{\pi}{9})}_{\mathbb{Q}(2\cos \pi/3) = \mathbb{Q}(\cos \pi/3)} : \mathbb{Q}] = 3$$

$\implies [\mathbb{Q}(\cos \pi/9) : \mathbb{Q}] = 3$ NOT a power of 2

8. Splitting Fields

Definition Splits

If $f \in F[x]$ and $F \subseteq E$ an extension then f **splits** in E when

$$f = \prod_{i=1}^{\deg(f)} (x - a_i)$$

where $a_i \in E$

By Corollary to Kronecker's theorem

$\exists$ an extension of F that contains that contains all the roots $a_1, a_2, \cdots, a_n$ $(n = \deg f)$ of f

If $\alpha_1, \alpha_2, \cdots, \alpha_d \in K$ roots of f then $E = F(\alpha_1, \cdots, \alpha_d)$

Splitting field

Definition

$f \in F[x]$ then the field

$$F(a_1, a_2, \cdots, a_n) \subseteq E$$

the extension containing all roots of f is called the **splitting field of f over F**

Example: $f = x^2 + 1$ has splitting field

$$\mathbb{Q}(i, -i) = \mathbb{Q}(i) \text{ over } \mathbb{Q}$$

Has splitting field $\mathbb{R}(i) = \mathbb{C}$ over $\mathbb{R}$

9. Groups Overview

- Groups
- Subgroups, Lagrange's theorem
- Cauchy's thm
- Subgroup Lattice $\mathcal{L}(G)$

10. Galois Groups

Automorphisms / Symmetries

Definition

A symmetry or automorphism of a field F is a map

$$\sigma : F \longrightarrow F$$

that is a bijection and

$$\sigma(a+b) = \sigma(a) + \sigma(b)$$

$$\sigma(ab) = \sigma(a)\sigma(b)$$

i.e. an isomorphism to itself.

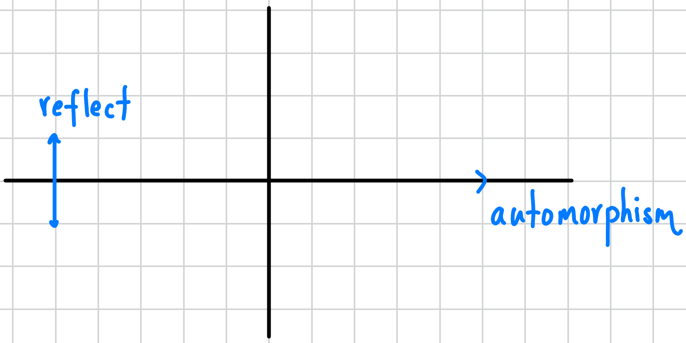
Example: Complex conjugation

$$\theta : \mathbb{C} \to \mathbb{C}$$

$$z \longmapsto \overline{z}$$

$$\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$$

$$\overline{z_1 z_2} = \overline{z}_1 \, \overline{z}_2$$



Example: $F \subseteq \mathbb{C}$

Then if $\frac{m}{n} \in \mathbb{Q}$:

$$\sigma\left(\frac{m}{n}\right) = \sigma\left(\frac{\overbrace{1+1+\cdots+1}^{m}}{\underbrace{1+1+\cdots+1}_{n}}\right)$$

$$= \sigma(\overbrace{1+\cdots+1}^{m})\,\sigma\left(\frac{1}{\underbrace{1+\cdots+1}_{n}}\right)$$

$$= (\sigma(1)+\cdots+\sigma(1)) \cdot \frac{1}{\sigma(1)+\cdots+\sigma(1)}$$

$$= 1+\cdots+1 \cdot \frac{1}{1+\cdots+1}$$

$$= \frac{m}{n}$$

Galois Groups

Definition

If $F \subseteq E$ are fields, then write

$$\mathrm{Gal}(E/F)$$

for the automorphism of E that fix F pointwise i.e.

$$\sigma(a) = a \qquad \forall a \in F$$

Exercise: $\mathrm{Gal}(E/F)$ is a group under composition of automorphism with the identity the identity automorphism

$$\sigma(a) = a \quad \forall a \in E$$

written "id" and σ^{-1} the usual inverse map

$$\boxed{\mathrm{Gal}(E/F) \text{ the Galois group of } E \text{ over } F}$$

Example: $F = \mathbb{Q}$

$E = \mathbb{Q}(\sqrt{2}, i)$ basis $\{1, i\}$

Here $\underbrace{\mathbb{Q} \subseteq \overbrace{\mathbb{Q}(\sqrt{2})}^{} \subseteq \mathbb{Q}(\sqrt{2}, i)}$

basis $\{1, \sqrt{2}\}$

$\xRightarrow[\text{law}]{\text{Tower}} \{1, \sqrt{2}, i, \sqrt{2}i\}$ basis for $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$

$$\Rightarrow \mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}i : a, b, c, d \in \mathbb{Q}\}$$

Then if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$

$$\sigma(a + b\sqrt{2} + ci + d\sqrt{2}i) = \sigma(a)\sigma(1) + \sigma(b)\sigma(\sqrt{2}) + \sigma(c)\sigma(i) + \sigma(d)\sigma(\sqrt{2}i)$$

$$= a + b\sigma(\sqrt{2}) + c\sigma(i) + d\sigma(\sqrt{2})\sigma(i)$$

elements of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}i)/\mathbb{Q})$ fixes rationals, $\mathbb{Q}$ by defn

$\Rightarrow \sigma$ completely determined by $\sigma(\sqrt{2})$ and $\sigma(i)$

This is a general fact.

$$\boxed{\text{If } F \subseteq F(\alpha_1, \dots, \alpha_k) = E, \text{ then } \sigma \in Gal(E/F) \text{ is completely determined by } \sigma(\alpha_1), \dots, \sigma(\alpha_k)}$$

For if $\{\beta_1, \dots, \beta_n\}$ a basis for E over F, then σ is completely determined by its effect on β_i

The proof of tower law gives

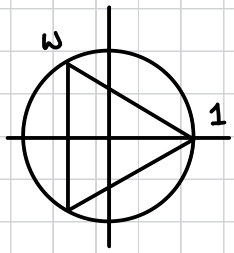
$$\beta_i = \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_k^{i_k}$$

a product of α_j's so that $\sigma(\beta_i) = \sigma(\alpha_1)^{i_1} \sigma(\alpha_2)^{i_2} \cdots \sigma(\alpha_k)^{i_k}$ is in turn determined by $\sigma(a_j)$'s

Example: Sometimes $Gal(E/F)$ can be computed by brute force

Consider $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ $\qquad \omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$

where $\omega^3 = 1$



Find min polynomial of ω over $\mathbb{Q}$

Guess 1: $x^3 - 1 = (x-1)(1+x+x^2)$ not irreducible

Guess 2: $1 + x + x^2$ ✓

$$\Rightarrow \mathbb{Q}(\omega) = \{a + b\omega : a, b \in \mathbb{Q}\} \text{ and } \omega^2 = -1 - \omega$$

If $\sigma \in Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ then σ determined by $\sigma(\omega)$ where

$$\sigma(\omega) = a + b\omega \quad \text{where } a, b \in \mathbb{Q}$$

Consider $\sigma(\omega^3)$

(i) $\sigma(\omega^3) = \sigma(1) = 1$

(ii) $\sigma(\omega^3) = \sigma(\omega)^3 = (a + b\omega)^3$

$$= a^3 + 3a^2 b\omega + 3a(b\omega)^2 + (b\omega)^3$$

$$= a^3 + 3a^2 b\omega + 3ab^2(-1-\omega) + b^3$$

$$= (a^3 + b^3 - 3ab^2) + (3a^2 b - 3ab^2)\omega$$

Equate 1 and ω parts

$$a^3 + b^3 - 3ab^2 = 1$$

$$3a^2 b - 3ab^2 = 0 \Rightarrow 3ab(a-b) = 0$$

$\Rightarrow a=0$ or $b=0$ or $a=b$

Hence $a=0 \Rightarrow b^3=1 \Rightarrow b=1$

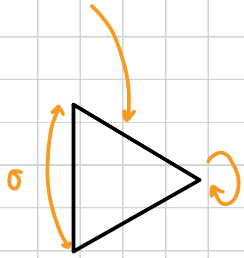
$b=0 \Rightarrow a^3=1 \Rightarrow a=1$

$a=b \Rightarrow a^3=-1 \Rightarrow a=-1=b$

$\Rightarrow \sigma(\omega)=\omega$, $\underbrace{\cancel{\sigma(\omega)=1}}$, $\sigma(\omega)=1-\omega$

σ bijection

$\Rightarrow Gal(\mathbb{Q}(\omega)/\mathbb{Q})=\{id, \sigma(\omega)=-1-\omega=\omega\}$



Extension Theorem

Theorem

Let F and K be fields

$\tau: F \longrightarrow K$ an isomorphism of fields

Also let α algebraic over F with minimum polynomial $f \in F[x]$

Finally let $\tau^*: F[x] \longrightarrow K[x]$ be the map

$$\tau^*\left(\sum a_i x^i\right)=\sum \tau(a_i)x^i$$

Then $\exists$ an isomorphism $\sigma: F(\alpha) \longrightarrow K(\beta)$ with

$$\sigma(\alpha)=\beta \iff \beta \text{ is a root of } \tau^* f$$

For us: let $F=K$, τ is the identity map

(hence τ^* is the identity too). This gives

So if α is algebraic over F with min polynomial $f \in F[x]$, then $\exists$ an isomorphism

$$\sigma: F(\alpha) \longrightarrow F(\beta) \text{ s t } \sigma(\alpha)=\beta \iff \beta \text{ is a root of } f.$$

If we also assume that $\beta \in F(\alpha)$ then you can show that (Ex) $F(\beta)=F(\alpha)$.

This gives

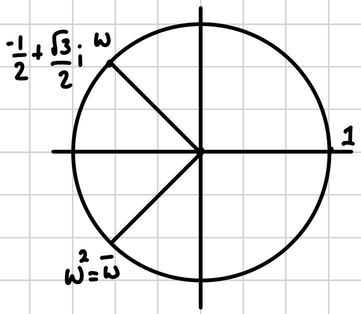
Corollary

If α algebraic over F with minimum polynomial f, then $\exists\, \sigma : F(\alpha) \longrightarrow F(\alpha)$ an isomorphism (i.e. an automorphism) with

$$\sigma(\alpha) = \beta \iff \beta \text{ is a root of } f \text{ that is contained in } F(\alpha)$$

Moral: Automorphisms of $F(\alpha)$ permute the roots of f, the min poly of α

Example: $\omega^3 = 1$. Finding $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$



Min poly of ω over $\mathbb{Q}$ is

$$1 + x + x^2$$

with roots ω and $\omega^2 = \bar{\omega}$

We get $\sigma \in Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ iff $\sigma(\omega)$ is one of these roots that is in $\mathbb{Q}(\omega)$

This gives $\sigma(\omega) = \omega$ or ω^2

As $\mathbb{Q}(\omega) = \{a + b\omega : a, b \in \mathbb{Q}\}$, thus

- if $\sigma(\omega) = \omega \implies \sigma(a + b\omega) = a + b\omega$, i.e. $\sigma = id$
- if $\sigma(\omega) = \omega^2 = \bar{\omega} \implies \sigma(a + b\omega) = a + b\bar{\omega}$

$$Gal(\mathbb{Q}(\omega)/\mathbb{Q}) = \{id, \sigma\}$$

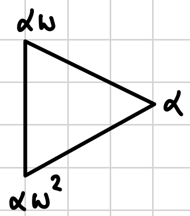
Example: $\alpha = \sqrt[3]{2} \in \mathbb{R}$. What is $Gal(\mathbb{Q}(\alpha), \mathbb{Q})$

Min poly over $\mathbb{Q}$ is

$$x^3 - 2 \qquad \text{Eisenstein}$$

with roots $\alpha, \alpha\omega, \alpha\omega^2$ where

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$$



But $\alpha\omega, \alpha\omega^2 \in \mathbb{C} \setminus \mathbb{R}$ but $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ so that

$$\alpha\omega, \alpha\omega^2 \notin \mathbb{Q}(\alpha)$$

Thus a $\sigma \in Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$ can only send α to α

As $\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}$ this gives $\sigma = id$

$$Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{id\}$$

Order of Galois group

Corollary Order Corollary

Let $f \in F[x]$ and E the splitting field of f over F. Moreover the roots of are distinct. Then:

$$|Gal(E/F)| = [E:F]$$

This formula: E and F are fields, hence rings and E is a vector space over F; also $Gal(E/F)$ is a group of automorphisms

Example: $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$

$$\alpha = \sqrt[3]{2}$$

On the otherhand, $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ is an extension of degree $= \deg(x^3-2)$

$$\text{i.e. } [\mathbb{Q}(\alpha):\mathbb{Q}] = 3$$

The splitting field of x^3-2 is $\mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2) \neq \mathbb{Q}(\alpha)$

Proposition

Let E be the splitting field over F of a polynomial with distinct roots. Suppose also that

$$E = F(\alpha_1, \dots, \alpha_m) \text{ for some } \alpha_1, \dots, \alpha_m \in E$$

such that

$$[E:F] = \prod_i [F(\alpha_i):F]$$

Then $\exists$ a $\sigma \in Gal(E/F)$ with $\sigma(\alpha_i) = \beta_i \iff \beta_i$ is a root of the minimum polynomial of α_i over F

Example: From section 0, we computed automorphisms of $\mathbb{Q}(\alpha, \omega)$ in an ad-hoc way.

$\alpha = \sqrt[3]{2}$, $\omega = \frac{-1}{2} + \frac{\sqrt{3}}{2} i$

Compute $|Gal(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})|$

(i) Claim $\mathbb{Q}(\alpha, \omega)$ is the splitting field of x^3-2 as the roots of this are $\alpha, \alpha\omega, \alpha\omega^2$

Then

$$\mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2) = \mathbb{Q}(\alpha, \omega)$$

(ii) Roots of x^3-2 are distinct

(iii) Compute $[\mathbb{Q}(\alpha,\omega):\mathbb{Q}]$

$$\underbrace{\mathbb{Q} \subseteq}_{(*)} \overbrace{\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha,\omega)}^{(**)}$$

(*) α has min poly x^3-2 over $\mathbb{Q}$

$\Longrightarrow [\mathbb{Q}(\alpha):\mathbb{Q}]=3$ Basis : $\{1,\alpha,\alpha^2\}$

(**) ω has min poly $1+x+x^2$ over $\mathbb{Q}(\alpha)$

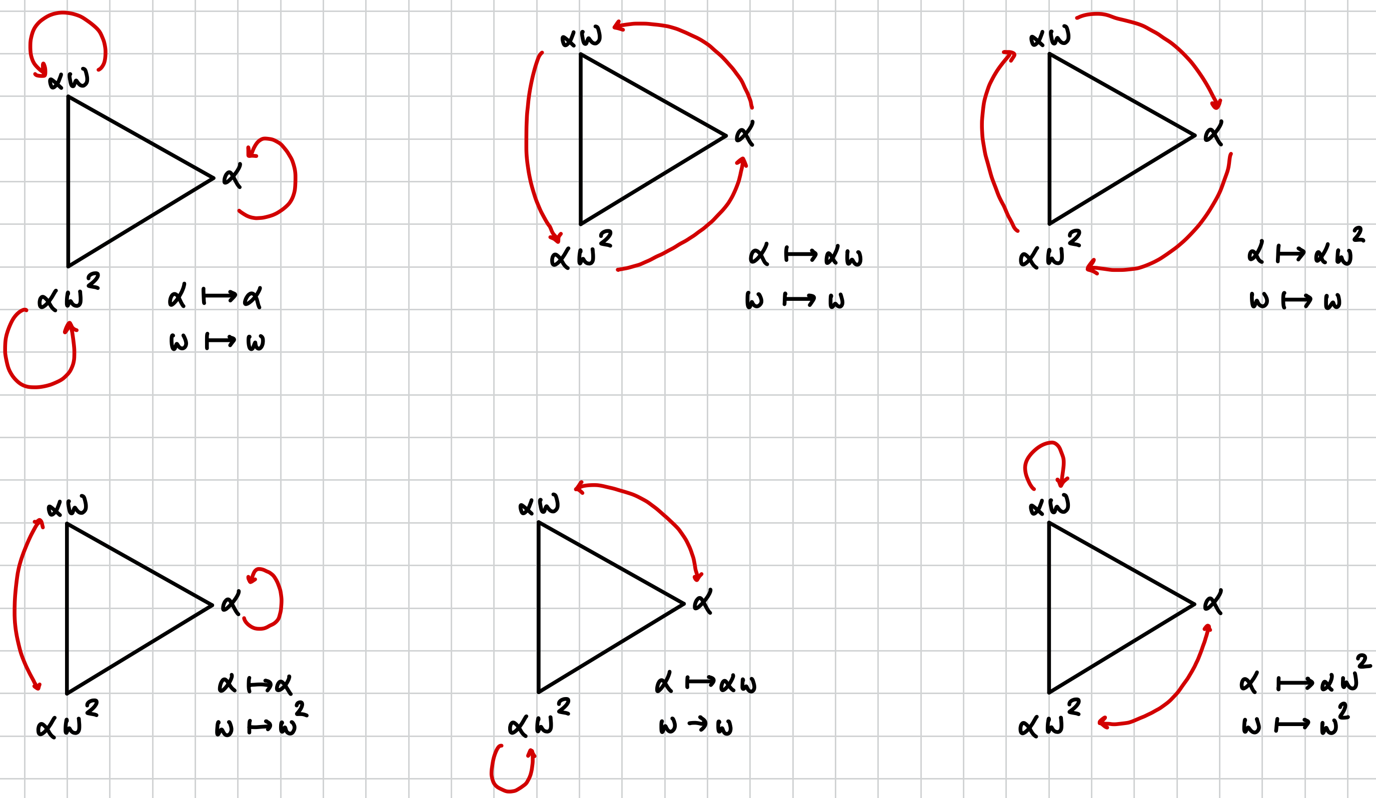
$\Rightarrow [\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\alpha)]=2$ Basis: $\{1,\omega\}$

$\Rightarrow [\mathbb{Q}(\alpha,\omega):\mathbb{Q}] = 2\times 3 = 6 = |\mathrm{Gal}(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})|$

$\{1,\alpha,\alpha^2,\omega,\alpha\omega,\alpha^2\omega\}$

Further by proposition above, we can send α to any of $\alpha, \alpha\omega, \alpha\omega^2$ and ω to any of ω, ω^2 and get an automorphism.

Following this through with the vertices of a triangle gives 3 automorphisms with ω mapped to itself and another 3 with ω mapped to ω^2



11. Fundamental Theorem of Galois Theory

We know that a complex number ς is constructible if $\exists$ a sequence of fields

$$\mathbb{Q} \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_m$$

such that $\mathbb{Q}(\varsigma) \subseteq k_m$ and each k_i is a degree 2 extension of k_{i-1} i.e. $[K_{i+1}.k_i] = 2$

To use this, we need to understand all the fields sandwiched between $\mathbb{Q}$ and $\mathbb{Q}(\delta)$

The Galois correspondence gives us this understanding

Definition Intermediate field

Let $F \subseteq E$ be an extension of fields and $F \subseteq K \subseteq E$

Call such a K an *intermediate field*

The *lattice of intermediate fields* consist of all such K s.t $k_1 \subseteq k_2$, then draw

$$\begin{tikzcd}[column sep=small] & k_2 \arrow[dl, dash] \\ k_1 & \end{tikzcd}$$

i.e.

$$\begin{tikzcd}[column sep=small] & E \arrow[d, dash] \\ & k_2 \arrow[dl, dash] \\ k_1 \arrow[dr, dash] & \\ & F \end{tikzcd}$$

$$F \subseteq k_1 \subseteq k_2 \subseteq E$$

compare with lattice of subgroups in Lecture # 15)

Notation: Write $\mathcal{L}(E/F)$ for this lattice

Theorem

If $F \subseteq E$ with

$$G = Gal(E/F)$$

and $\mathcal{L}(G)$ the lattice of all subgroups of G and $\mathcal{L}(E/F)$ the lattice of intermediate fields

Then

(i) H a subgroup of $G = Gal(E/F)$ then

$$E^H = \{\lambda \in E : \sigma(\lambda) = \lambda \ \ \forall \sigma \in H\}$$

is an intermediate field called the fixed field of H

(ii) if K is an intermediate field then $Gal(E/K)$ is a subgroup of

$$G = Gal(E/F)$$

(iii) The maps $\Psi : H \longrightarrow E^H$ and $\Phi : K \rightarrow Gal(E/K)$ are mutual inverses hence bijections

$$\Psi . \mathcal{L}(G) \rightleftarrows \mathcal{L}(E/F) : \Phi$$

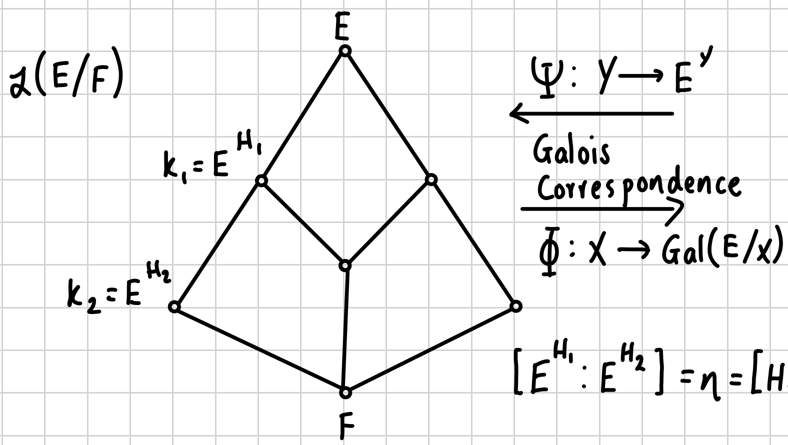
that reverse order i.e.

$$H_1 \subseteq H_2 \xrightarrow{\Psi} E^{H_2} \subseteq E^{H_1}$$

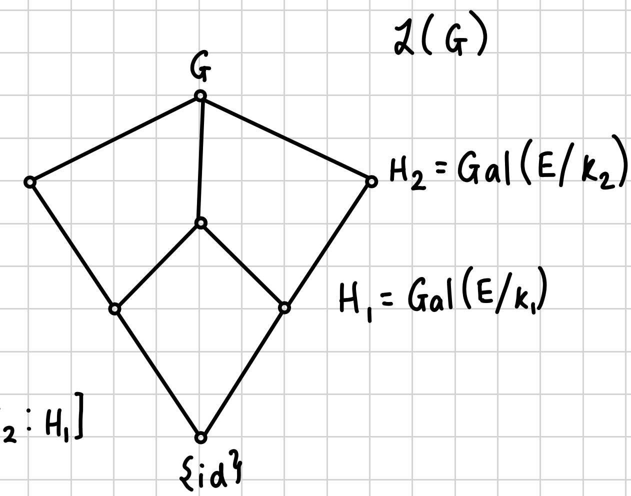
$$K_2 \subseteq K_1 \xrightarrow{\Phi} Gal(E/K_1) \subseteq Gal(E/K_2)$$

(iv) The degree of $E^H \subseteq E$ is equal to the order of $|H|$ or the degree of $F \subseteq E^H$ is equal to the index $[G : H]$

Schematically



$$[E^{H_1} : E^{H_2}] = n = [H_2 : H_1]$$



Why upside down? If $H_1 \in \mathcal{L}(G)$ then $E^{H_1} = \{\lambda \in E \mid \sigma(\lambda) = \lambda \ \ \forall \sigma \in H_1\}$

And $H_1 \subseteq H_2$ then E^{H_2} are these elements fixed by all the $\sigma \in H_2$.

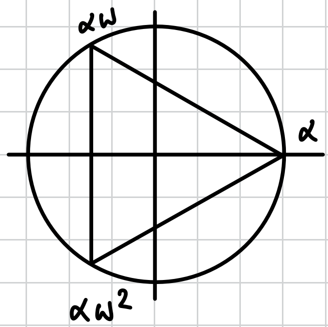
Thus E^{H_2} is the result of imposing more conditions on E^{H_2}. hence smaller

Example: $F=\mathbb{Q}$

$$E=\mathbb{Q}(\underbrace{\sqrt[3]{2}}_{\alpha},\ \underbrace{-1/2+\sqrt{3}/2\, i}_{\omega}) \qquad \alpha^3=2$$

$\omega=1$

Remember x^3-2 has roots



Consider $Gal(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})$; suppose that $\sigma,\tau\in Gal(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})$ such that

$$\sigma(\alpha)=\alpha\omega \qquad \sigma(\omega)=\omega$$

$$\tau(\alpha)=\alpha \qquad \tau(\omega)=\omega^2$$

$\Rightarrow \{id, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ —— (*) are also in $Gal(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})$

	id	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
α	α	$\alpha\omega$	$\alpha\omega^2$	α	$\alpha\omega$	$\alpha\omega^2$
ω	ω	ω	ω	ω^2	ω^2	ω^2

$\sigma^2(\alpha)=\sigma(\sigma(\alpha))$
$=\sigma(\alpha\omega)=\sigma(\alpha)\sigma(\omega)=\alpha\omega\cdot\omega=\alpha\omega^2$

Thus (*) gives 6 distinct elements of $Gal(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})$

Moreover from order corollary, we have

$$|Gal(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})| = [\mathbb{Q}(\alpha,\omega):\mathbb{Q}]$$

Recall: $\mathbb{Q}(\alpha,\omega)=\mathbb{Q}(\alpha,\alpha\omega,\alpha\omega^2)$ the splitting field of x^3-2. Also

$$\underbrace{\mathbb{Q}\subseteq\mathbb{Q}(\alpha)}_{\text{basis }\{1,\alpha,\alpha^2\}}\subseteq\mathbb{Q}(\alpha,\omega)$$

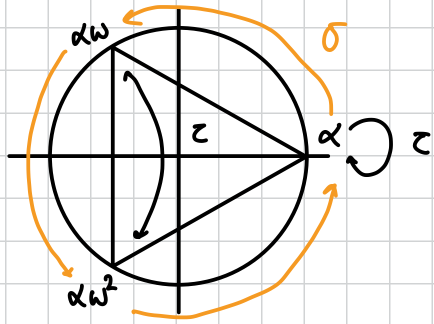
basis $\{1,\omega\}$

$\Rightarrow \{1,\alpha,\alpha^2,\omega,\alpha\omega,\alpha^2\omega\}$ basis for $\mathbb{Q}(\alpha,\omega)$ over $\mathbb{Q}$

Thus $Gal(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})=\{id,\sigma,\sigma^2,\tau,\sigma\tau,\sigma^2\tau\}$

What is the subgroup lattice of $\mathcal{L}(G)$?

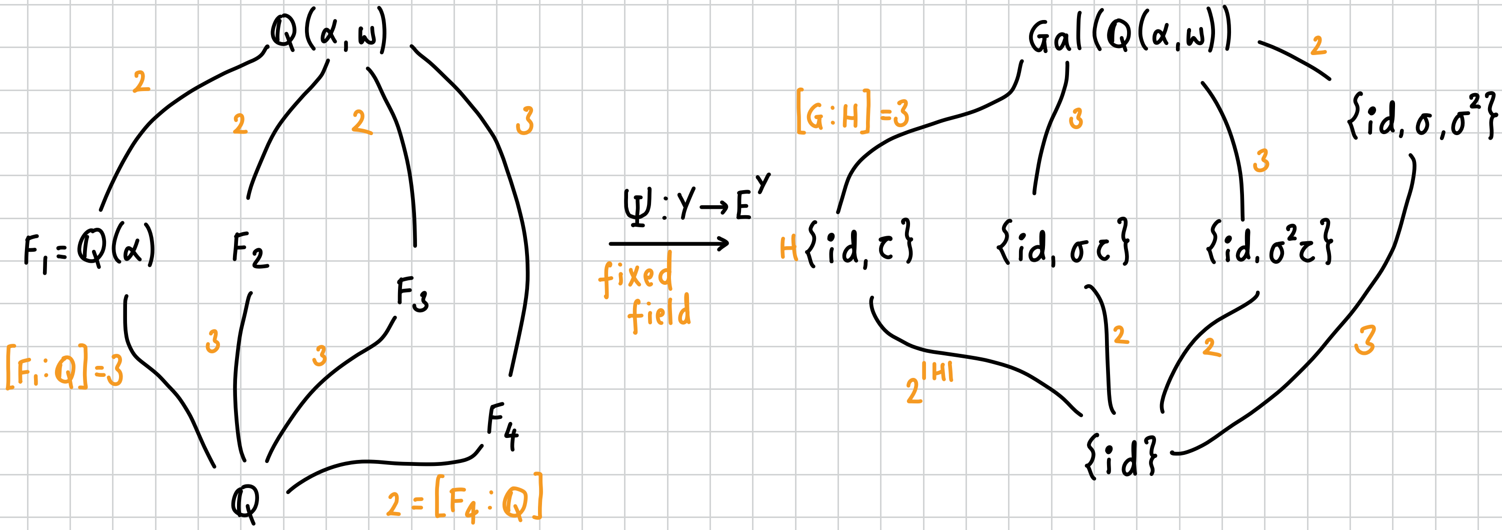
$G = Gal(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})$



These give geometric symmetries

This gives our first picture

$\mathcal{L}(\mathbb{Q}(\alpha,\omega),\mathbb{Q})$ $\qquad\qquad$ $\mathcal{L}(Gal(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})$



Find F_1 = fixed field of $H = \{id, \tau\}$

$= \mathbb{Q}(\alpha,\omega)^{\{id,\tau\}}$

A typical element of $\mathbb{Q}(\alpha,\omega)$ is

$$x = a_0 + a_1\alpha + a_2\alpha^2 + a_3\omega + a_4\alpha\omega + a_5\alpha^2\omega \qquad a_1,\dots,a_5 \in \mathbb{Q}$$

We want those x s.t $id(x) = x$ and $\tau(x) = x$ $\quad$ by defn of fixed field of H

$$\tau(x) = a_0 + a_1\alpha + a_2\alpha^2 + a_3\omega^3 + a_4\alpha\omega^2 + a_5\alpha^2\omega^2$$

$(1+\omega+\omega^2 = 0$ since min poly of ω is $f = 1 + x + x^2)$

$$= a_0 + a_1\alpha + a_2\alpha^2 + a_3(-1-\omega) + a_4\alpha(-1-\omega) + a_5\alpha^2(-1-\omega)$$

$$= (a_0 - a_3) + (a_1 - a_4)\alpha + (a_2 - a_5)\alpha^2 - a_3\omega - a_4\alpha\omega - a_5\alpha^2\omega$$

For $\tau(x) = x$, equate coefficients

$$\left.\begin{array}{l|l} a_0 - a_3 = a_0 & a_0 = a_0 \quad\quad -a_3 = a_3 \\ a_1 - a_4 = a_1 & a_1 = a_1 \quad\quad -a_4 = a_4 \\ a_2 - a_5 = a_2 & a_2 = a_2 \quad\quad -a_5 = a_5 \end{array}\right\} \Rightarrow a_3 = a_4 = a_5 = 0$$

Thus $\tau(x) = x \iff x = a_0 + a_1\alpha + a_2\alpha^2$

i.e. $x \in \mathbb{Q}(\alpha)$

i.e $F_1 \subseteq \mathbb{Q}(\alpha)$

But τ fixes $\mathbb{Q}$ and $\tau(\alpha) = \alpha \Rightarrow \tau$ fixes $\mathbb{Q}(\alpha)$

$\Rightarrow \mathbb{Q}(\alpha) \subseteq F_1$

since $\mathbb{Q}(\alpha)$ smallest field

$\Rightarrow F_1 = \mathbb{Q}(\alpha)$

11. (Not) Solving Equations

You know: ax^2+bx+c has roots $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$

Can you do this in general ???

Radical Extension

Definition

A extension $\mathbb{Q}\subseteq E$ is a radical when $\exists$ a sequence of simple extensions

$$\mathbb{Q}\subseteq \mathbb{Q}(\alpha_1)\subseteq \mathbb{Q}(\alpha_1,\alpha_2)\subseteq\cdots\subseteq \mathbb{Q}(\alpha_1,\dots,\alpha_k)=E$$

where each α_i is s.t $\alpha_i^{m_i}\in\mathbb{Q}(\alpha_1,\dots,\alpha_{i-1})$ for some power $m_i\in\mathbb{Z}^{\geq 0}$

i.e. α_i is an m_i-th root of an element of $\mathbb{Q}(\alpha_1,\dots,\alpha_{m_{i-1}})$

Example:

$$\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})\subseteq\mathbb{Q}(\sqrt{2},\sqrt[3]{5})\subseteq\mathbb{Q}\left(\sqrt{2},\sqrt[3]{5},\sqrt{\sqrt{2}+3\sqrt{5}}\right)$$

Definition Solvable by radicals

A polynomial is solvable by radicals iff its splitting field is contained in some radical extension

Example: any $ax^2+bx+c\in\mathbb{Q}[x]$ is solvable by radicals as its splitting field is contained in

$$\mathbb{Q}\left(\sqrt{b^2-4ac}\right)$$

a radical extension.

Similarly for cubics, quartics

Definition

The Galois group of $f\in\mathbb{Q}[x]$ is the Galois group

$$\mathrm{Gal}(E/\mathbb{Q})$$

where E is the splitting field of E

Theorem Galois

$f \in \mathbb{Q}[x]$ is solvable by radicals

$$\Updownarrow$$

The Galois group of f is soluble*

$\boxed{S_n \text{ NOT soluble for } n \geq 5}$

Example: $x^5 - 4x + 2$ not solvable by radicals

(i.e. there is no formula for the roots of $x^5 - 4x + 2$)

For let
$$E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$$
be the splitting field of f with $\alpha_1, \alpha_2, \dots, \alpha_5$ the roots. Then
$$\alpha_i^5 - 4\alpha_i + 2 = 0$$

If $\sigma \in Gal(E/\mathbb{Q})$ then
$$\sigma(\alpha_i^5 - 4\alpha_i + 2) = \sigma(0) \implies \sigma(\alpha_i)^5 - 4\sigma(\alpha_i) + 2 = 0$$
$$\implies \sigma(\alpha_i) \text{ is also a root of } f$$
$$\implies Gal(E/\mathbb{Q}) \text{ permutes the roots of } f$$
$$\implies Gal(E/\mathbb{Q}) \text{ is isomorphic to a subgroup of } S_5$$

Moreover $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq \mathbb{Q}(\alpha_1, \dots, \alpha_5) = E \underset{\text{Law}}{\overset{\text{Tower}}{\implies}} [E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha_1) : \mathbb{Q}]$

where the min poly of α_1 over $\mathbb{Q}$ is $x^5 - 4x + 2$ (irred by Eisenstein)

$$\implies [\mathbb{Q}(\alpha_i) : \mathbb{Q}] = 5$$
$$\implies 5 \text{ divides } [E : \mathbb{Q}]$$

We also know:

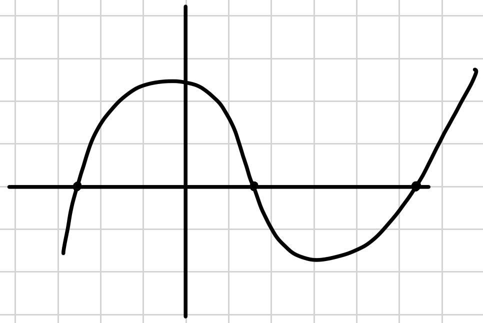
splitting field
$$|Gal(E/\mathbb{Q})| = [E : \mathbb{Q}]$$

Thus 5 divides $|Gal(E/\mathbb{Q})| \underset{\text{Thm}}{\overset{\text{Cauchy}}{\implies}} Gal(E/\mathbb{Q})$ has subgroup $\{id, \sigma, \sigma^2, \sigma^3, \sigma^4\}$ of order 5

Thus $\exists\, \sigma \in Gal(E/\mathbb{Q})$ of form $\sigma = (a, b, c, d, e)$ where $a, b, c, d, e \in \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$

Also complex conjugation $\tau : z \mapsto \bar{z}$ is an automorphism of $\mathbb{C}$ and this restricted to E to give an element of $Gal(E/\mathbb{Q})$

In fact f looks like



i.e. three roots of are real hence two are complex conjugates

Thus τ is a permutation of (b_1, b_2)

(c.f : every element of S_n can be written in terms of (12)
$(12 \cdots n)$)

Similarly every element of S_5 can be written in terms of σ and $\tau \Rightarrow Gal(E/\mathbb{Q}) \cong S_5$
insoluble

$\Rightarrow$ f not solvable by radicals