1. introduction

Equation

$$a_0x^n + a_1x_{n-1} + \ldots + a_{n-1}x + a_n = 0.$$

where $a_0 \neq 0$ is called general algebraic equation in 1 variable of degree n

1.1. Solve 3rd degree equation (Cardano Solution)

$$x^3 + ax^2 + bx + c = 0. \tag{1}$$

take $x = y + d$ where $d = -\frac{a}{3}$ equation (1) become

$$x^3 + px + q = 0.$$

take $y_0 = \alpha + \beta$ to be a solution of equation (?) where α, β undetermined. We get

$$\alpha^3 + \beta^3 + (\alpha + \beta)(3\alpha\beta + p) + q = 0$$

If we can set $3\alpha\beta + p = 0$ then

$$\{ \begin{aligned} \alpha^3 + \beta^3 &= -q \\ \alpha^3\beta^3 &= -\frac{p^3}{27} \end{aligned} .$$

So α^3, β^3 are solutions of $x^2 + qx - \frac{p^3}{27} = 0$

$$\begin{aligned} y_{1,2,3} = {} & \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \\ & \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\omega} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\omega^2} \\ & \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\omega^2} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\omega}. \end{aligned}$$

notice $\alpha\beta$ fixed.

1.2. Solve 4th degree equation (Ferrari)

$$x^4+ax^3+bx^2+cx+d=0. \tag{2}$$

Take $y=x+\frac{a}{4}$

$$y^4+py^2+qy+r=0.$$

Transform

$$\left(y^2+\frac{p}{2}\right)^2+qy+\left(r-\frac{p^2}{4}\right)=0.$$

and

$$\left(y^2+\frac{p}{2}+\alpha\right)^2-\left(2\alpha\left(y^2+\frac{p}{2}\right)+\alpha^2-qy-r+\frac{p^2}{4}\right)=0.$$

where α is arbitrary, choose α to make $2\alpha\left(y^2+\frac{p}{2}\right)+\alpha^2-qy-r+\frac{p^2}{4}$ a perfect square.

to let discriminant $q^2-8\alpha\left(\alpha p+\alpha^2-r+\frac{p^2}{4}\right)=0$. It is a 3rd degree equation of α, which is solvoble. Take any one of the root, we can factorize (?)to 4 1st degree equations.

Another way of solution(Geometrical):

$$y^4+py^2+qy+r=0.$$

Assume $u=y^2$, then equivalently solve a pair of equations:

$$\begin{cases} u-y^2=0 \\ u^2+pu+qy+r=0 \end{cases}$$

Assume a quadratic form $Q=A\begin{pmatrix} 0 & 0 & \frac{1}{2} \\ 0 & -1 & 0 \\ \frac{1}{2} & 0 & 0 \end{pmatrix}+B\begin{pmatrix} 1 & 0 & \frac{p}{2} \\ 0 & 0 & \frac{q}{2} \\ \frac{p}{2} & \frac{q}{2} & r \end{pmatrix}$,

Let $\det(Q)=0$, solve the 3rd degree eqation for $\frac{A}{B}$, give 3 solutions, corresponding to 3 pairs of lines(degenerate conics), then calculate the intersection of line pairs give the 4 roots.

1.3. Abel's theorem

For general ≥ 5 degree equation, there is no fomula for solution w.r.t coefficients involving operations of adding, subtracting, multiplication, division, raising to a natural degree and extraction of roots of a natural degree.

2. Groups

2.1. Composite of operation

Example 2.1 *Operation over numbers. a) addition b)subtraction c)multiplication over 1)even natural number 2) odd natural number 3) negative integer.*

1. Binary operation over set.
2. Ordered pair and Catesian product of sets.
3. Extention of number system.

Example 2.2 *Rotation in equilateral triangle.* $< \sigma|\sigma^3 = e >$, $\sigma = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$

1. Permutation representation.
2. Multiplication table.

Example 2.3 *All symmetries of a) equilateral triangle. b) square c) rectangle d) rhombus.*

2.2. Transformation groups

Example 2.4 $\varphi(x) = x+1,\ \varphi(x) = 2x,\ \varphi(x) = -x,\ \varphi(x) = -2x+1, \varphi(x) = \frac{1}{x},$
$\varphi(t) = v_0 t + \frac{1}{2} g t^2,\ \varphi(t) = (\cos t,\ \sin t),\ \varphi(n) = \{ \begin{matrix} 3n+1 & n\ odd \\ n/2 & n\ even \end{matrix} ,$
$\varphi(n) = 4n \bmod 7,\ \varphi(n) = n^2 \bmod 5,\ \varphi : \begin{matrix} [n] \to [n] \\ i \mapsto \varphi(i) \end{matrix}$

1. Mapping $\varphi : M \to N$, injective, surjective, bijective. composition of mapping.
2. Transformation $\varphi : M \to M$, identity transformation, inverse transformation φ^{-1}.
3. Associativity.
4. Transformation group. (cyclic group, dihedral group, translation group, rotation group, rigid motion group, primitive root mod p)
5. Commutativity?

2.3. Formal definition of groups

Example 2.5 *Conter-examples of group a)*$(\mathbb{R} \setminus \{0\}, +)$, *b)*$(\mathbb{N}^*, \times)$,

1. Identity element is unique.
2. Inverse element is unique.
3. $\left(a^{-1}\right)^{-1} = a$.
4. $(ab)^{-1} = b^{-1}a^{-1}$

Example 2.6 *Free group* $< B, W, B^{-1}, W^{-1} >$

1. Word, concatenation, plain word.

Example 2.7 $< B, W|B^3 = 1, W^2 = 1, BW = WB >$

$< B, W | B^3 = 1, W^2 = 1, BW = WB^2 >$

1. Generator, Relator

Example 2.8 *There are n markers, each with one side white and the other side black, aligned in a row so that their white sides are up. In each step, if possible, we choose a marker with the white side up (but not one of the outermost markers), remove it and reverse the closest marker to the left and the closest marker to the right of it.*
Prove that one can achieve the state with only two markers remaining if and only if n−1 is not divisible by 3.

Example 2.9 *Three Reflection Theorem: Any isometry of $\mathbb{R}^2$ is a combination of one, two, or three reflections.*

2.4. Cyclic groups

1. order of element
2. definition of cyclic group.(generated by 1 element)
3. $a^m = e$ iff $\operatorname{ord}(a) | m$

Example 2.10 *Find the generator of 1)Rotation group of equilateral triangle 2)Square 3)Regular n-polygon 4)$(\mathbb{Z}, +)$ 5)$((\mathbb{Z}/p\mathbb{Z})^*, \times)$*

2.5. Isomorphisms

1. Definition of isomorphism $G \xrightarrow{\varphi} H$, bijection and $\forall a, b \in G\ \varphi(a)\varphi(b) = \varphi(ab)$
2. φ is isomorphism then φ^{-1} is isomorphism
3. $\varphi_1 : A \to B$ and $\varphi_2 : B \to C$ is isomorphism, then $\varphi_2 \circ \varphi_1$ is isomorphism
4. φ keeps identity and inverse.

2.5.1. Cayley Theorem

1. $\varphi_a : x \mapsto ax$ is an isomorphism
2. prove Cayley theorem

$$\begin{aligned} \psi : G &\to LG \\ a &\mapsto \varphi_a \end{aligned}$$

2.6. Subgroups

$H \leq G$ iff H is 1) closed under multiplication of G. 2) contains the unit. 3) contains the inverse.

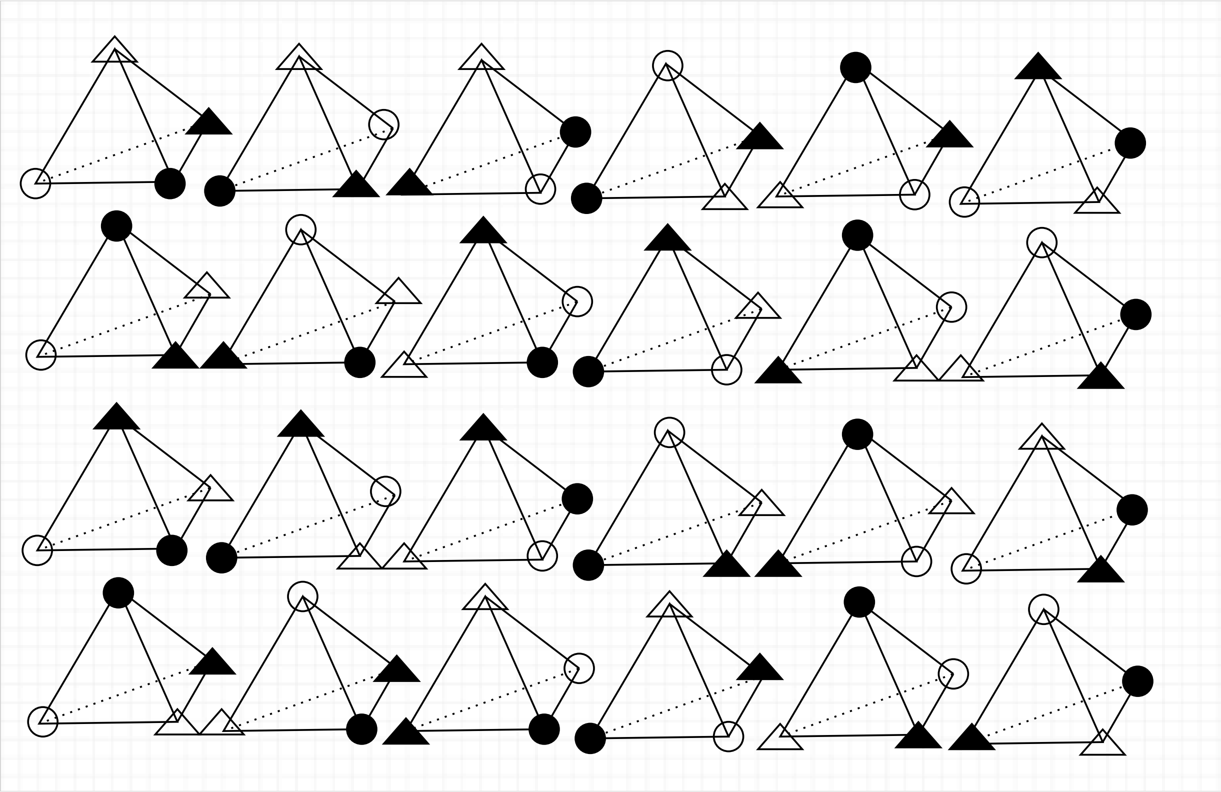
Example 2.11 *Find all subgroups of a)symmetry group of equilateral triangle. b)symmetry group of square. c)$\mathbb{Z}_3$ d)$\mathbb{Z}_8$ e)$\mathbb{Z}_{15}$ f)infinite cyclic group*

Solution: a)$A_3 = C_3 \leq S_3 = D_3,\ C_2 \leq S_3$
b)$C_4, C_2, \mathbb{Z}_2 \oplus \mathbb{Z}_2 = K$
c)trivial d)$\mathbb{Z}_2, \mathbb{Z}_4$ e)$\mathbb{Z}_3, \mathbb{Z}_5$
f)$\{np | n \in \mathbb{Z}\}$ Bezout Theorem.

Example 2.12 *Symmetry group of tetrahedron and subgroups.*

1)Elements $\begin{pmatrix} A & B & C & D \\ B & C & A & D \end{pmatrix}\begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}\begin{pmatrix} A & B & C & D \\ A & C & B & D \end{pmatrix}\begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}$

2)Subgroup isomorphic to a)symmetry of triangle. b)cyclic $\mathbb{Z}_4$ c)all rotations(preserving orientation. d).cyclic $\mathbb{Z}_2, \mathbb{Z}_3$ as subgroup of all rotations.



Remark: Cayley graph $G(S_4; (12), (13), (14))$ truncated hexahedron.

2.7. Direct product

1. $G \times H$ is a group..
2. If $G_1 \le G, H_1 \le H$ then $G_1 \times H_1 \le G \times H$.

Example 2.13 $K \le G \times H$ *implys* $K = G_1 \times H_1$*?*

Solution: $<(1,1)> \le \mathbb{Z}_3 \times \mathbb{Z}_6$ an conterexample.

Example 2.14 *Prove that a)$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. b)$\mathbb{Z}_2^n \cong \mathbb{Z}_{2^n}$*

Solution:a)Chinese remainder theorem b)wrong. consider order of element.

2.7.1. Chinese remainder theorem

2.8. Cosets

1. Given $H \le G, g \in G$,call gH the left coset.

2. Non-intersection Union of cosets.

2.8.1. Lagrange Order Theorem

1. Order of subgroup.
2. Order of element.

2.8.2. Eular Theorem

2.8.3. Existence of Primitive Root(a)

Lemma 1 ***If*** $\mathrm{ord}(a) = m, \mathrm{ord}(b) = n,\ \gcd(m, n) = 1,$ ***then*** $\mathrm{ord}(ab) = mn$

proof of lemma: $ord(ab) = r|mn$, $a^{rn} \equiv (ab)^{rn} \equiv 1$, so $ord(a) = m|rn$, so $m|r$.
Similarly $n|r$. Then $mn|r$.
proof of theorem: suppose $\mathrm{ord}(a) = m, \mathrm{ord}(b) = n,\ \gcd(m, n) = l,\ m = m'l,\ n = n'l$
then $\mathrm{ord}\left(a^l\right) = m'$ and $\mathrm{ord}\left(b^l\right) = n'$,

by lemma $\mathrm{ord}\left(b^l a\right) = n'm = \mathrm{lcm}(m, n)$.

If M is the maximal order, then $\forall a\ \mathrm{ord(a)}|M$, so $x^M - 1 = 0$ has $p - 1$ elements. Contradict with Lagrange polynomial theorem.

2.8.4. Existence of Primitive Root(b)

Denote $\psi(d)$ the number of elements with order d

$$\sum_{d|p-1} \psi(d) = p - 1$$

$$\sum_{d|n} \varphi(d) = n$$

For any d,
If $\psi(d) > 0$, suppose $\mathrm{ord}(a) = d$, and $n_1, n_2,\ \ldots n_{\varphi(d)}$ are numbers relatively prime to d, then a^{n_i} will also has order d. And solutions of $x^d - 1 = 0$ are exactly $\left\{1, a,\ \ldots a^{d-1}\right\}$ by Lagrange theorem. So $\psi(d) = \varphi(d)$.
Else $\psi(d) = 0$

$$\sum_{d|p-1} \psi(d) \le \sum_{d|p-1} \varphi(d)$$

When $n = p - 1$, we get $\psi(d) = \varphi(d)$.

2.8.5. Structure of $((\mathbb{Z}/n\mathbb{Z})^*, \times)$

$(\mathbb{Z}/n\mathbb{Z})^*, \times)$ is cyclic Iff $n = p^\alpha, 2p^\alpha, 2, 4\ (p\ odd\ prime)$.

1, $\left(\mathbb{Z}/p^e\mathbb{Z}\right)^*$ $is\ cyclic\ (p\ odd\ prime)$

proof: take $g^{p-1} \equiv 1\ (mod\ p)$ and $g^{p-1} \not\equiv 1\ \left(mod\ p^2\right)$ (by Lagrange theorem,

then $g^{p-1} = 1 + ap,\ (a,p) = 1.\ (1+ap)^{p^{e}} = g^{p^{e} - p^{e-1}} \equiv 1\left(mod\ p^{e}\right)$ by Eular theorem.
so $ord(g) | \varphi\left(p^{e}\right) = p^{e} - p^{e-1}$.
prove the following by induction $ord_{p^{k}}(1+ap) = p^{k-1}$ becase $(1+ap)^{p^{k-1}} \equiv 1 + \lambda p^{k}\left(mod\ p^{k+1}\right)$ where $(\lambda, p) = 1$.
prove $ord_{p^{e}}(g) = \varphi\left(p^{e}\right) = p^{e} - p^{e-1} = p^{e-1}(p-1)$
if $g^{n} \equiv 1\left(mod\ p^{e}\right)$ then $g^{n} \equiv 1\left(mod\ p^{e-1}\right)$, by induction hypothesis $ord_{p^{e-1}}(g) = p^{e-2}(p-1)|n$
suppose $n = p^{e-2}(p-1)n'$ then $g^{n} \equiv (1+ap)^{p^{e-2}\ n'}\left(mod\ p^{e}\right)$ so $ord_{p^{e}}(1+ap)|p^{e-2}n'$,
then $p^{e-1}(p-1)|n$, so $ord_{p^{e}}(g) = p^{e-1}(p-1)$
2) $(\mathbb{Z}/2\mathbb{Z})^{*}$,$(\mathbb{Z}/4\mathbb{Z})^{*}$ cyclic.
3) $\left(\mathbb{Z}/p_1^{e_1}\mathbb{Z}\right)^{*} \times \left(\mathbb{Z}/p_2^{e_2}\mathbb{Z}\right)^{*} \cong \left(\mathbb{Z}/p_1^{e_1} \cdot p_2^{e_2}\mathbb{Z}\right)^{*}$ not cyclic.
proof: $\varphi\left(p_1^{e_1}\right) = p_1^{e_1} - p_1^{e_1 - 1}$ and $\varphi\left(p_2^{e_2}\right) = p_2^{e_2} - p_2^{e_2 - 1}$ are even except p^{e}=2. So has 2 different order 2 element. Which can not be cyclic.
4)$\left(\mathbb{Z}/2p^{e}\mathbb{Z}\right)^{*} \cong \left(\mathbb{Z}/2p^{e}\mathbb{Z}\right)^{*}$ cyclic
5)$\left(\mathbb{Z}/2^{n}\mathbb{Z}\right)^{*} \cong \left\{2^{a}5^{b} | a = 0,1;\ b = 0,1,\ \dots, 2^{e-2} - 1\right\} \cong (\mathbb{Z}/2\mathbb{Z},\ +) \oplus \left(\mathbb{Z}/2^{e-2}\mathbb{Z},\ +\right)$

proof: $5^{b} + 1 = (4+1)^{b} + 1 = 2 + \sum_{k=1}^{b} C_b^k 4^k,$

$5^{b} - 1 = (4+1)^{b} - 1 = \sum_{k=1}^{b} C_b^k 4^k$,

$2^{\lambda+2} || 5^{b} - 1$ If $b = 2^{\lambda}$, so $2^{e} | 5^{b} - 1$ as $2^{e-2} | b$.

2.9. Inner automorphism

GIven transformation $f : S \rightarrow S$. After relabeling the elements by $T : S \rightarrow S$. φ become a new transformation of $f : S \rightarrow S$. Where T acts as a transformation of $\mathrm{Aut}(S)$.

Example 2.15 $f = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$, $T = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$, *draw the new transformation.*

$$\begin{tikzcd} A \arrow[r, mapsto, "f"] \arrow[d, "T"'] & f(A) \arrow[d, "T"] \\ T(A) \arrow[r, rightsquigarrow] & T(f(A)) \end{tikzcd}$$

Define $\varphi : \begin{matrix} \mathrm{Aut}(S) \times \mathrm{Aut}(S) \rightarrow \mathrm{Aut}(S) \\ (T, f) \mapsto \varphi_T(f) \end{matrix}$, where $\varphi_T : \begin{matrix} \mathrm{Aut}(S) \rightarrow \mathrm{Aut}(S) \\ f \mapsto T \circ f \circ T^{-1} \end{matrix}$ is called an inner automorphism.
In general given a group G and $g \in G$, denote inner automorphism by $\varphi_g \in \mathrm{Aut}(G)$, where

$\varphi_h : \begin{array}{c} G \to G \\ g \mapsto hgh^{-1} \end{array}$. Check all the inner automorphism forms a group isomorphic to G itself.

Example 2.16 *Find pairs of elements can be sent to each other by inner automorphisms:*
a)symmetry of equilateral triangle D_3
b)symmetry of regular tetrahedron S_4
c)rotation of regular tetrahedron A_4

Example 2.17 *Conjugation of subgroup $H \leq G$ by $g \in G$, i.e. $\varphi_g(G) = gGg^{-1}$ is a subgroup of G.*

T.F.A.E: giver $H \leq G$
a) $\forall g \in G, \forall h \in H,\ \varphi_g(h) \in H$.
b) $\forall g \in G,\ \varphi_g(H) = H.$.
c) $\forall g \in G, gH = Hg$.
Then $H \lhd G$ is called normal subgroup.

2.10. Normal subgroups

Example 2.18 $<(1\ 2)> \leq D_3,\ <(1\ 2\ 3)> \lhd D_3$

Example 2.19 *Find normal subgroup of D_4.*

2.11. Cayley Graph

2.12. Quotient groups

Example 2.20 $D_4 / \{e, a\} \cong K_4$*? where a is the $180°$ rotation of square and K_4 is symmetry group of rhombus i.e. Klein 4 group.*

Example 2.21 *Find all normal subgroups and the quotient group of a)D_3 b)$\mathbb{Z}_2 \times \mathbb{Z}_2$ c)$(\mathbb{Z}, +)$ d)$(\mathbb{Z}_n, +)$ e)D_4 f) Quarternions*
e)Rotation of tetrahedron A_4

Example 2.22 $G_1 \cong G_1 \times e_2 \lhd G_1 \times G_2$.

2.13. Commutator

Definition: Finite product of commutators obtain a normal subgroup.

$$K(G) =< [a, b] > \quad = \{[a_1, b_1][a_2, b_2] \ldots [a_k, b_k]\}$$

where $[a, b] = aba^{-1}b^{-1}$for some $a, b \in G$.

Example 2.23 *Find the commutator in a)symmetry group of triangle. b)symmetry group of triangle. c)group of Quatenion. d)symmetry group of regular n-gon. e)symmetry group of tetrahedron. f)rotation group of a cube or octahedron.*

Example 2.24 *Prove a)G/N is abelian group iff $K(G) \leq N \lhd G$*
b)If $N \lhd G$ then $K(N) \lhd G$

2.14. Homomorphisms

Example 2.25 *Homomorphism from symmetry group of square to symmetry of rhombus. Considering the permutation of the 4 axis of the sqaure.*

Example 2.26 *Homomorphism from rotation group of cube to $\mathbb{Z}_2$. Where $\mathbb{Z}_2$ denote the permutation of the two tetrahedron inscribed in cube.*

2.15. Natural homomorphism

2.15.1. Kernal and Image

2.15.2. Normal subgroup in surjective homomorphism

$$\pi : G \to G/N$$

a) For $N \lhd G$, the projection map $\pi : G \to G/N$ is homomorphism.
b) For surjective homomorphism $\varphi : G \to H$, $\psi : G/ker\varphi \to H$ is an induced isomorphism.

Example 2.27 *a)Quotient group of $R/\mathbb{Z}_n$,where R is the plane rotation group fixing 0, $\mathbb{Z}_n$ is the rotation group of regular n-gon.*

Example 2.28 *$\varphi : G \to F$ surjective homomorphism,K_1, K_2 is commutator of G, F. a) Prove $\varphi(K_1) = K_2$, b) Is it true $K_1 = \varphi^{-1}(K_2)$.*

2.16. Solvable groups

Definition: G is solvoble iff the sequence $G, K(G), K_2(G) \dots$ end (i.e. for some finite n, $K_n(G) = \{e\}$)
where $K(G)$ denote the commutator of G, $K_{r+1}(G) = K(K_r(G))$.

2.16.1. Example of solvable groups

problem159

2.16.2. Dodecahedron

problem160-164 non-solvable

2.16.3. Solution Sequence

problem165-174
$G, K(G), K_2(G) \dots$ is normal sequence and also characteristic, i.e. $K_i(G) \rhd K_j(G) \dots$
Definition of characteristic subgroup: $K \leq H$ is a characteristic subgroup iff $\forall \varphi : H \to H$ automorphism, $\varphi(K) \subset K$.
If $K \leq H$ is characteristic (implies $K \lhd H$) and $H \lhd G$ then $K \lhd G$

2.17. Permutations

2.17.1. Solvablity of S_4 and Cayley graph

2.17.2. Non-solvability of S_5 and Dodachahedron

problem 192-196

3. Complex Numbers

The 'existence' (or ontology) in mathematical creatures serves as intuition for Platoniasm, or neglected for pragmatism.

3.1. Fields and polynomials

3.1.1. Operations

3.2. Field of complex numbers

3.3. Uniqueness

minimal field extension

3.4. Geometric description

3.5. Trigonometric form

3.6. Continuity

3.6.1. $\epsilon - \delta$ language

3.7. Curve

winding number

3.8. Fundamental theorem of algebra

3.9. Riemann surface diagram of $\omega = \sqrt{z}$

branch point

3.10. Riemann Surface of more complicated functions

Due to classification of oriented Riemann surface, all the examples can be draw globally by compactification.
Here understand intuitionally or going deep to complex analysis and algebraic curve.