Math is Fun & Beautiful! - Abstract Algebra

Sunghee Yun
sunghee.yun@gmail.com

Table of contents

- table of contents - 1
- kinds of fun we can enjoy with math - 2
- notations - 3
- some definitions - 6
- some conventions - 7
- selected proofs - 139
- index - 149

Kinds of fun we can enjoy with math

- abstract algebra 8
  - groups 12, rings 51, polynomials 73
  - algebraic extensions 90, Galois theory 123

Notations

- sets of numbers
  - **N**: set of natural numbers, **Z**: set of integers, **Q**: set of rational numbers
  - **R**: set of real numbers, $\mathbf{R}_+$: set of nonnegative real numbers, $\mathbf{R}_{++}$: set of positive real numbers
- sequences $\langle x_i \rangle$ and like
  - finite $\langle x_i \rangle_{i=1}^n$, infinite $\langle x_i \rangle_{i=1}^\infty$ - use $\langle x_i \rangle$ when unambiguously understood
  - similarly for other operations - $\sum x_i$, $\prod x_i$, $\cup A_i$, $\cap A_i$, $\bigtimes A_i$
  - similarly for integrals - $\int f$ for $\int_{-\infty}^{\infty} f$
- sets
  - $\tilde{A}$: complement of A, $A \sim B$: $A \cap \tilde{B}$, $A \Delta B$: $A \cap \tilde{B} \cup \tilde{A} \cap B$
  - $\mathcal{P}(A)$: set of all subsets of A
- sets in metric vector spaces
  - $\overline{A}$: closure of set A
  - A°: interior of set A
  - $\mathbf{relint}$: relative interior of set A

  - $\mathbf{bd}\, A$: boundary of set A
- set algebra
  - $\sigma(\mathcal{A})$: σ-algebra generated by $\mathcal{A}$, $i.e.$, smallest σ-algebra containing $\mathcal{A}$
- norms in $\mathbf{R}^n$
  - $\|x\|_p$ $(p \geq 1)$: p-norm of $x \in \mathbf{R}^n$, $i.e.$, $(|x_1|^p + \cdots + |x_n|^p)^{1/p}$
  - $\|x\|_2$: Euclidean norm
- matrices and vectors
  - a_i: i-th entry of vector a
  - A_{ij}: entry of matrix A at position (i, j), $i.e.$, entry in i-th row and j-th column
  - $\mathbf{Tr}(A)$: trace of $A \in \mathbf{R}^{n \times n}$, $i.e.$, $A_{1,1} + \cdots + A_{n,n}$
- symmetric, positive definite, and positive semi-definite matrices
  - $\mathbf{S}^n \subset \mathbf{R}^{n \times n}$: set of symmetric matrices
  - $\mathbf{S}^n_+ \subset \mathbf{S}^n$: set of positive semi-definite matrices - $A \succeq 0 \Leftrightarrow A \in \mathbf{S}^n_+$
  - $\mathbf{S}^n_{++} \subset \mathbf{S}^n$: set of positive definite matrices - $A \succ 0 \Leftrightarrow A \in \mathbf{S}^n_{++}$
- Python script-like notations (with serious abuse of notations!)

- use $f : \mathbf{R} \to \mathbf{R}$ as if it were $f : \mathbf{R}^n \to \mathbf{R}^n$, $e.g.$,

$$\exp(x) = (\exp(x_1), \ldots, \exp(x_n)) \quad \text{for } x \in \mathbf{R}^n$$

  or

$$\log(x) = (\log(x_1), \ldots, \log(x_n)) \quad \text{for } x \in \mathbf{R}^n_{++}$$

  corresponding to Python code - `numpy.exp(x)` or `numpy.log(x)` - where `x` is instance of `numpy.ndarray`, $i.e.$, `numpy` array
- use $\sum x$ for $\mathbf{1}^T x$ for $x \in \mathbf{R}^n$, $i.e.$

$$\sum x = x_1 + \cdots + x_n$$

  corresponding to Python code - `x.sum()` - where `x` is `numpy` array
- use x/y for $x, y \in \mathbf{R}^n$ for

$$\begin{bmatrix} x_1/y_1 & \cdots & x_n/y_n \end{bmatrix}^T$$

  corresponding to Python code - `x / y` - where `x` and `y` are 1-d `numpy` arrays
  - applies to any two matrices of same dimensions

Some definitions

Definition 1. [infinitely often - i.o.] *statement, P_n, said to happen* infinitely often *or* i.o. *if*

$$(\forall N \in \mathbf{N})\,(\exists n > N)\,(P_n)$$

Definition 2. [almost everywhere - a.e.] *statement, $P(x)$, said to happen* almost everywhere *or* a.e. *or* almost surely *or* a.s. *(depending on context) associated with measure space, $(X, \mathscr{B}, \mu)$ if*

$$\mu\{x|P(x)\} = 1$$

or equivalently

$$\mu\{x| \sim P(x)\} = 0$$

Some conventions

- for some subjects, use following conventions
  - $0 \cdot \infty = \infty \cdot 0 = 0$
  - $(\forall x \in \mathbf{R}_{++})(x \cdot \infty = \infty \cdot x = \infty)$
  - $\infty \cdot \infty = \infty$

Abstract Algebra

Why Abstract Algebra? & Some Historical View

Why abstract algebra?

- first, it's fun!

- and, lets us understand instrict structures of algebraic objects

- and, doing it allows us to solve *extremely practical problems*; well, depends on your definition of practicality
  - $e.g.$, can prove why not exist general root formulas for polynomials of order greater than 4 - is it practical enough for you?

- also prepare us for pursuing further math topics such as differential geometry, algebraic geometry, analysis, representation theory, algebraic number theory, $etc.$

- and ... it's really fun; sheer examination and pondoring upon ideas make us happy and thrilled!

Some history

- by the way, historically, often the case that application of an idea presented before extracting and presenting the idea on its own right

- $e.g.$, Galois used "quotient group" only implicitly in his 1830's investigation, and it had to wait until 1889 to be explicitly presented as "abstract quotient group" by Hölder

Groups

Monoids

Definition 3. [law of composition] *mapping $S \times S \to S$ for set S, called* law of composition (of S to itself)

- *when $(\forall x, y, z \in S)((xy)z = x(yz))$, composition is said to be* associative
- *$e \in S$ such that $(\forall x \in S)(ex = xe = x)$, called* unit element *- always unique*
  Proof: for unit elements, e, f $e = ef = f$, hence, $e = f$

Definition 4. [monoids] *set, M, with composition which is associative and having unit element, called* monoid *(so in particular, M is not empty)*

- *monoid, M, with $(\forall x, y \in M)\,(xy = yx)$, called* commutative or abelian *monoid*
- *subset, $H \subset M$, which has element and is itself monoid, called* submonoid

Groups

Definition 5. [groups] *monoid, G, with*

$$(\forall x \in G)\,(\exists y \in G)\,(xy = yx = e)$$

called group

- *for $x \in G$, $y \in G$ with $xy = yx = e$, called* inverse of x
- *group derived from commutative monoid, called* abelian group *or* commutative group
- *group, G, with $|G| < \infty$, called* finite group
- *(similarly as submonoid) $H \subset G$ that has unit element and is itself group, called* subgroup
- *subgroup consisting only of unit element, called* trivial

Cyclic groups, generators, and direct products

Definition 6. [cyclic groups] *group, G, with*

$$(\exists a \in G)\,(\forall x \in G)\,(\exists n \in \mathbf{N})\,(x = a^n)$$

called cyclic group, *such $a \in G$, called* cyclic generator

Definition 7. [generators] *for group, G, $S \subset G$ with*

$$(\forall x \in G)\,(x \textit{ is arbitrary product of elements or inverse elements of } S)$$

called set of generators for G, *said to* generate G, *denoted by* $G = \langle S \rangle$

Definition 8. [direct products] *for two groups, G_1 and G_2, group, $G_1 \times G_2$, with*

$$(\forall (x_1, x_2), (y_1, y_2) \in G_1 \times G_2)\,((x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2, y_2) \in G_1 \times G_2)$$

whose unit element defined by (e_1, e_2) where e_1 and e_2 are unit elements of G_1 and G_2 respectively, called direct product of G_1 and G_2

Homeomorphism and isomorphism

Definition 9. [homeomorphism] *for monoids, M and M', mapping $f : M \to M'$ with $f(e) = e'$*

$$(x, y \in M)\,(f(xy) = f(x)f(y))$$

where e and e' are unit elements of M and M' respectively, called monoid-homeomorphism *or simple* homeomorphism

- group homeomorphism, *$f : G \to G'$, is similarly monoid-homeomorphism*
- *homeomorphism, $f : G \to G'$ where exists $g : G \to G'$ such that $f \circ g : G' \to G'$ and $g \circ f : G \to G$ are identity mappings,called* isomorphism, *sometimes denoted by $G \approx G'$*
- *homeomorphism of G into itself, called* endomorphism
- *isomorphism of G onto itself, called* automorphism

- set of all automorphisms of G is itself group, denoted by $\mathrm{Aut}(G)$

Kernel, image, and embedding of homeomorphism

Definition 10. [kernels of homeomorphism] *for group-homeomorphism, $f : G \to G'$, where e' is unit element of G', $f^{-1}(\{e'\})$, which is subgroup of G, called* kernel of f, *denoted by* $\mathrm{Ker}\ f$

Definition 11. [embedding of homeomorphism] *homeomorphism, $f : G \to G'$, establishing isomorphism between G and $f(G) \subset G'$, called* embedding

Proposition 1. [group homeomorphism and isomorphism]

- *for group-homeomorphism, $f : G \to G'$, $f(G) \subset G'$ is subgroup of G'*
- *homeomorphism whose kernel is trivial is injective, often denoted by special arrow*

$$f : G \hookrightarrow G'$$

- *surjective homeomorphism whose kernel is trivial is* isomorphism
- *for group, G, its generators, S, and another group, G', map, $f : S \to G'$ has at most one extension to homeomorphism of G into G'*

Orthogonal subgroups

Proposition 2. [orthogonal subgroups] *for group, G, and two subgroups, $H, K \subset G$, with $HK = G$, $H \cap K = \{e\}$, and $(x \in H, y \in K)\,(xy = yx)$,*

$$f : H \times K \to G$$

with $(x, y) \mapsto xy$ is isomorphism

can generalize to finite number of subgroups, $H_1, \ldots, H_n$ such that

$$H_1 \cdots H_n = G$$

and

$$H_{k+1} \cap (H_1 \cdots H_k) = \{e\}$$

in which case, G is isomorphic to $H_1 \cdots H_n$

Cosets of groups

Definition 12. [cosets of groups] *for group, G, and subgroup, $H \subset G$, aH for some $a \in G$, called left coset of H in G, and element in aH, called coset representation of aH - can define right cosets similarly*

Proposition 3. [cosets of groups] *for group, G, and subgroup, $H \subset G$,*

- *for $a \in G$, $x \mapsto ax$ induces bijection of H onto aH, hence all left cosets have same cardinality*
- *$aH \cap bH \neq \emptyset$ for $a, b \in G$ implies $aH = bH$*
- *hence, G is disjoint union of left cosets of H*
- *same statements can be made for right cosets*

Definition 13. [index and order of groups] *number of left cosets of H in G, called index of H in G, denoted by $(G : H)$ - index of trivial subgroups, called order of G, denoted by $(G : 1)$*

Indices and orders of groups

Proposition 4. [indices and orders] *(proof can be found in Proof 1) for group, G, and two subgroups, $H, K \subset G$ with $K \subset H$,*

$$(G : H)(H : K) = (G : K)$$

when K is trivial, we have

$$(G : H)(H : 1) = (G : 1)$$

hence, if $(G : 1) < \infty$, both $(G : H)$ and $(H : 1)$ divide $(G : 1)$

Normal subgroup

Definition 14. [normal subgroups] *subgroup, $H \subset G$, of group, G, with*

$$(\forall x \in G)\,(xH = Hx) \Leftrightarrow (\forall x \in G)\left(xHx^{-1} = H\right)$$

called normal subgroup of G*, in which case*

- *set of cosets, $\{xH|x \in G\}$, is with law of composition defined by $(xH)(yH) = (xy)H$, forms group with unit element, H, denoted by G/H, called* factor group of G by H*, read* G modulo H *or* G mod H
- *$x \mapsto xH$ induces homeomorphism of X onto $\{xH|x \in G\}$, called* canonical map*, kernel of which is H*

Proposition 5. [normal subgroups and factor groups]

- *kernel of (every) homeomorphism of G is normal subgroups of G*
- *for family of normal subgroups of G, $\langle N_\lambda \rangle$, $\bigcap N_\lambda$ is also normal subgroup*
- *every subgroup of abelian group is normal*
- *factor group of abelian group is abelian*
- *factor group of cyclic group is cyclic*

Normalizers and centralizers

Definition 15. [normalizers and centralizers] *for subset, $S \subset G$, of group, G,*

$$\{x \in G | xSx^{-1} = S\}$$

is subgroup, called normalizer of S, *and also called* centralizer of a *when $S = \{a\}$ is singletone;*

$$\{x \in G | (\forall y \in S)(xyx^{-1} = y)\}$$

called centralizer of S, *and centralizer of G itself, called* center of G

- *e.g.*, $A \mapsto \det A$ of multiplicative group of square matrices in $\mathbf{R}^{n \times n}$ into $\mathbf{R} \sim \{0\}$ is homeomorphism, kernel of which called *special linear group,* and (of course) is normal

Normalizers and congruence

Proposition 6. [normalizers of groups] *subgroup, $H \subset G$, of group, G, is normal subgroup of its normalizer, N_H*

- *subgroup, $H \subset G$, of group, G, is normal subgroup of its normalizer, N_H*
- *subgroup, $K \subset G$ with $H \subset K$ where H is normal in K, is contained in N_H*
- *for subgroup, $K \subset N_H$, KH is group and H is normal in KH*
- *normalizer of H is largest subgroup of G in which H is normal*

Definition 16. [congruence with respect to normal subgroup] *for normal subgroup, $H \subset G$, of group, G, we write*

$$x \equiv y \pmod{H}$$

if $xH = yH$, read x and y are congruent modulo H - this notation used mostly for additive groups

Exact sequences of homeomorphisms

Definition 17. [exact sequences of homeomorphisms] *below sequence of homeomorphisms with* $\operatorname{Im} f = \operatorname{Ker} g$

$$G' \xrightarrow{f} G \xrightarrow{g} G''$$

said to be exact

below sequence of homeomorphisms with $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \longrightarrow \cdots \xrightarrow{f_{n-1}} G_n$$

said to be exact

- for normal subgroup, $H \subset G$, of group G, sequence, $H \xrightarrow{j} G \xrightarrow{\varphi} G/H$, is exact where j is inclusion and φ
- $0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$ is exact *if and only if* f injective, g surjective, and $\operatorname{Im} f = \operatorname{Ker} g$

- if $H = \operatorname{Ker} g$ above, $0 \to H \to G \to G/H \to 0$
- more precisely, exists commutative diagram as in figure, in which vertical mappings are isomorphisms and rows are *exact*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G' & \xrightarrow{f} & G & \xrightarrow{g} & G'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G/H & \longrightarrow & 0 \end{array}$$

Canonical homeomorphism examples

all homeomorphisms described below called *canonical*

- for two groups, G and G', and homeomorphism, $f : G \to G'$, whose kernel is H, exists unique homeomorphism $f_* : G/H \to G'$ with

$$f = f_* \circ \varphi$$

  where $\varphi : G \to G/H$ is canonical map, and f_* is injective
  - f_* can be defined by $xH \mapsto f(x)$
  - say *f_* is induced by f*
  - f_* induces isomorphism, $\lambda : G/H \to \operatorname{Im} f$
  - below sequence summarizes above statements

$$G \xrightarrow{\varphi} G/H \xrightarrow{\lambda} \operatorname{Im} f \xrightarrow{j} G$$

  where j is inclusion

- for group, G, subgroup, $H \subset G$, intersection of all normal subgroups containing H, N ($i.e.$, smallest normal subgroup containing H), homeomorphism, $f : G \to G'$ whose kernel contains H, $N \subset \mathrm{Ker}\, f$ and exists unique homeomorphism, $f_* : G/N \to G'$ such that

$$f = f_* \circ \varphi$$

  where $\varphi : G \to G/H$ is canonical map

  - f_* can be defined by $xN \mapsto f(x)$
  - say *f_* is induced by f*

- for subgroups of G, H and K, with $K \subset H$, $xK \mapsto xH$ induces homeomorphism of G/K into G/H, whose kernel is $\{xK | x \in H\}$, thus *canonical isomorphism*

$$(G/K)/(H/K) \approx (G/K)$$

  this can be shown in figure where rows are exact

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G/H & \longrightarrow & 0 \\ & & \downarrow \text{can} & & \downarrow \text{can} & & \downarrow \text{id} & & \\ 0 & \longrightarrow & H/K & \longrightarrow & G/K & \longrightarrow & G/H & \longrightarrow & 0 \end{array}$$

- for subgroup, $H, K \subset G$, with H contained in normalizer of K, $H \cap K$ is normal subgroup of H, $HK = KH$ is subgroup of G, exists surjective homeomorphism

$$H \to HK/K$$

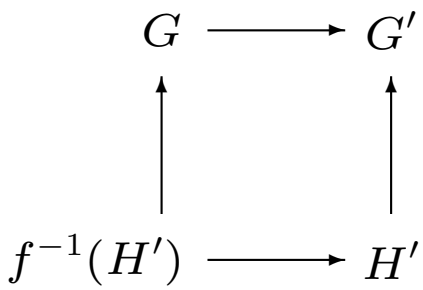
with $x \mapsto xK$, whose kernel is $H \cap K$, hence *canonical isomorphism*

$$H/(H \cap K) \approx HK/K$$

- for group homeomorphism, $f : G \to G'$, normal subgroup of G', H',

$$H = f^{-1}(H') \subset G$$

as shown in figure,



H is normal in G and kernel of homeomorphism

$$G \xrightarrow{f} G' \xrightarrow{\varphi} G'/H'$$

is H where φ is canonical map, hence we have injective homeomorphism

$$\bar{f} : G/H \to G'/H'$$

again called *canonical homeomorphism*, giving commutative diagram in figure; if f is surjective, $\bar{f}$ is isomorphism

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G/H & \longrightarrow & 0 \\ & & \downarrow & & \downarrow f & & \downarrow \bar{f} & & \\ 0 & \longrightarrow & H' & \longrightarrow & G' & \longrightarrow & G'/H' & \longrightarrow & 0 \end{array}$$

Towers

Definition 18. [towers of groups] *for group, G, sequence of subgroups*

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m$$

called tower of subgroups, called normal if every G_{i+1} is normal in G_i, called abelian if normal and every factor group G_i/G_{i+1} is abelian, called cyclic if normal and every factor group G_i/G_{i+1} is cyclic

Proposition 7. [towers inded by homeomorphism] *for group homeomorphism, $f : G \to G'$ and normal tower*

$$G' = G'_0 \supset G'_1 \supset G'_2 \supset \cdots \supset G'_m$$

tower

$$f^{-1}(G') = f^{-1}(G'_0) \supset f^{-1}(G'_1) \supset f^{-1}(G'_2) \supset \cdots \supset f^{-1}(G'_m)$$

is

- *normal if G'_i form normal tower*

- *abelian if G_i' form abelian tower*
- *cyclic if G_i' form cyclic tower*

because every homeomorphism

$$G_i/G_{i+1} \to G_i'/G_{i+1}'$$

is injective

Refinement of towers and solvability of groups

Definition 19. [refinement of towers] *for tower of subgroups, tower obtained by inserting finite number of subgroups, called* refinement of tower

Definition 20. [solvable groups] *group having an abelian tower whose last element is trivial subgroup, said to be* solvable

Proposition 8. [finite solvable groups]

- *abelian tower of finite group admits cyclic refinement*
- *finite solvable group admits cyclic tower, whose last element is trivial subgroup*

Theorem 1. [Feit-Thompson theorem] *group whose order is prime power is solvable*

Theorem 2. [solvability condition in terms of normal subgroups] *for group, G, and its normal subgroup, H, G is solvable* if and only if *both H and G/H are solvable*

Commutators and commutator subgroups

Definition 21. [commutator] *for group,* G, $xyx^{-1}y^{-1}$ *for* $x, y \in G$, *called* commutator

Definition 22. [commutator subgroups] *subgroup generated by commutators of group,* G, *called* commutator subgroup, *denoted by* G^C, $i.e.$

$$G^C = \langle \{xyx^{-1}y^{-1} | x, y \in G\} \rangle$$

- G^C is normal in G
- G/G^C is commutative
- G^C is contained in kernel of every homeomorphism of G into commutative group
- (proof can be found in Proof 2) for proof of above statements

- *commutator group is at the heart of solvability and non-solvability problems!*

Simple groups

Definition 23. [simple groups] *non-trivial group having no normal subgroup other than itself and trivial subgroup, said to be* simple

Proposition 9. [simple groups] *abelian group is simple* if and only if *cycle of prime order*

Butterfly lemma

Lemma 1. [butterfly lemma - Zassenhaus] *for subgroups, U and V, of group, and normal subgroups, u and v, of U and V respectively,*

$$u(U \cap v) \text{ is normal in } u(U \cap V)$$

$$(u \cap V)v \text{ is normal in } (U \cap V)v$$

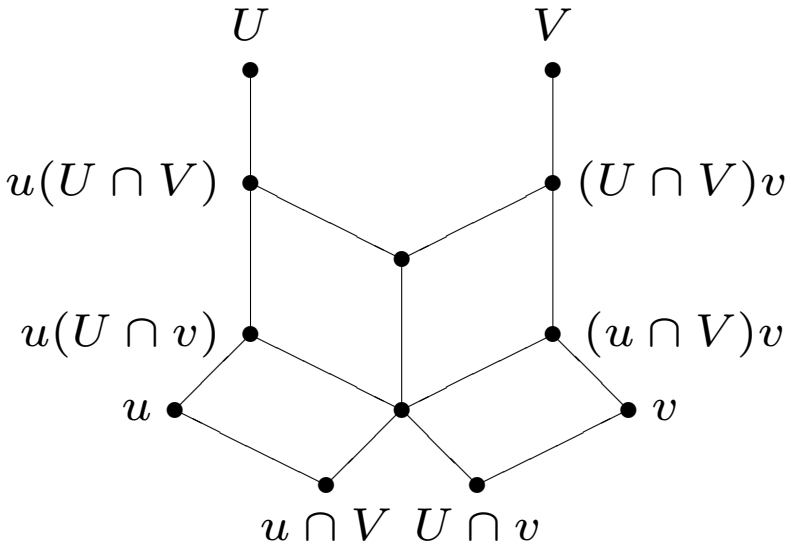
and factor groups are isomorphic, $i.e.$

$$u(U \cap V)/u(U \cap v) \approx (U \cap V)v/(u \cap V)v$$

these shown in figure

- indeed,

$$(U \cap V)/((u \cap V)(U \cap v)) \approx u(U \cap V)/u(U \cap v) \approx (U \cap V)v/(u \cap V)v$$


U
V
$u(U \cap V)$
$(U \cap V)v$
$u(U \cap v)$
$(u \cap V)v$
u
v
$u \cap V$
$U \cap v$

Equivalent towers

Definition 24. [equivalent towers] *for two normal towers of same height starting from same group ending with trivial subgroup*

$$G = G_1 \supset G_2 \supset G_3 \supset \cdots \supset G_{n+1} = \{e\}$$

$$G = H_1 \supset H_2 \supset H_3 \supset \cdots \supset H_{n+1} = \{e\}$$

with

$$G_i/G_{i+1} \approx H_{\pi(i)+1}/H_{\pi(i)}$$

for some permutation $\pi \in \mathrm{Perm}(\{1, \ldots, n\})$, *i.e., sequences of factor groups are same up to isomorphisms and permutation of indices, said to be* equivalent

Schreier and Jordan-Hölder theorems

Theorem 3. [Schreier] *two normal towers starting from same group and ending with trivial subgroup have equivalent refinement*

Theorem 4. [Jordan-Hölder theorem] *all normal towers starting from same group and ending with trivial subgroup where each factor group is non-trivial and simple are equivalent*

Cyclic groups

Definition 25. [exponent of groups and group elements] *for group, G, $n \in \mathbf{N}$ with $a^n = e$ for $a \in G$, called* exponent of a*; $n \in \mathbf{N}$ with $x^n = e$ for every $x \in G$, called* exponent of G

Definition 26. [period of group elements] *for group, G, and $a \in G$, smallest $n \in \mathbf{N}$ with $a^n = e$, called* period of a

Proposition 10. [period of elements of finite groups] *for finite group, G, of order, $n > 1$, period of every element, $a \neq e$, devided n; if n is prime number, G is cyclic, and period of every generator is p*

Proposition 11. [subgroups of cyclic groups] *every subgroup of cyclic group is cyclic and image of every homeomorphism of cyclic group is cyclic*

Properties of cyclic groups

Proposition 12. [properties of cyclic groups]

- *infinity cyclic group has exactly two generators; if a is one, a^{-1} is the other*
- *for cyclic group, G, of order, n, and generator, x, set of generators of G is*

$$\{x^m | m \text{ is relatively prime to } n\}$$

- *for cyclic group, G, and two generators, a, b, exists automorphism of G mapping a onto b; conversely, every automorphism maps a to some generator*
- *for cyclic group, G, of order, n, and $d \in \mathbf{N}$ dividing n, exists unique subgroup of order, d*
- *for cyclic groups, G_1 and G_2, of orders, n and m respectively with n and m relatively prime, $G_1 \times G_2$ is cyclic group*
- *for non-cyclic finite abelian group, G, exists subgroup isomorphic to $C \times C$ with C cyclic with prime order*

Symmetric groups and permutations

Definition 27. [symmetric groups and permutations] *for nonempty set, S, group G, of bijective functions of S onto itself with law of composition being function composition, called* symmetric group of S, *denoted by* $\mathrm{Perm}(S)$; *elements in* $\mathrm{Perm}(S)$ *called* permutations of S; *element swapping two disjoint elements in S leaving every others left, called* transposition

Proposition 13. [sign homeomorphism of finite symmetric groups] *for finite symmetric group, S_n, exits unique homeomorphism $\epsilon : S_n \to \{-1, 1\}$ mapping every transposition, τ, to -1, i.e., $\epsilon(\tau) = -1$*

Definition 28. [alternating groups] *element of finite symmetric group, σ, with $\epsilon(\sigma) = 1$, called* even, *element, σ, with $\epsilon(\sigma) = -1$, called* odd; *kernel of ϵ, called* alternating group, *denoted by* A_n

Theorem 5. [solvability of finite symmetric groups] *symmetric group, S_n with $n \geq 5$ is* not *solvable*

Theorem 6. [simplicity of alternating groups] *alternating group, A_n, with $n \geq 5$ is simple*

Operations of group on set

Definition 29. [operations of group on set] *for group, G, and set, S, homeomorphism,*

$$\pi : G \to \mathrm{Perm}(S)$$

called operation of G on S *or* action of G on S

- *S, called G-set*
- *denote $\pi(x)$ for $x \in G$ by π_x, hence homeomorphism denoted by $x \mapsto \pi_x$*

- obtain mapping from such operation, $G \times S \to S$, with $(x, s) \mapsto \pi_x(s)$
- often abbreviate $\pi_x(s)$ by xs, with which two properties satisfied
  - $(\forall x, y \in G, s \in S)\,(x(ys) = (xy)s)$
  - $(\forall s \in S)\,(es = s)$
- conversely, for mapping, $G \times S \to S$ with $(x, s) \mapsto xs$ satisfying above two properties, $s \mapsto xs$ is permutation for $x \in G$, hence π_x is homeomorphism of G into $\mathrm{Perm}(S)$
- thus, operation of G on S can be defined as mapping, $S \times G \to S$, satisfying above two properties

Conjugation

Definition 30. [conjugation of groups] *for group, G, and map, $\gamma_x : G \to G$ with $\gamma_x(y) = xyx^{-1}$, homeomorphism*

$$G \to \mathrm{Aut}(G) \text{ defined by } x \mapsto \gamma_x$$

called conjugation*, which is operation of G on itself*

- γ_x, called *inner*
- kernel of conjugation is *center of G*
- to avoid confusion, instead of writing xy for $\gamma_x(y)$, write

$$\gamma_x(y) = xyx^{-1} = {}^{x}y \text{ and } \gamma_{x^{-1}}(y) = x^{-1}yx = y^{x}$$

- for subset, $A \subset G$, map, $(x, A) \mapsto xAx^{-1}$, is operation of G on set of subsets of G
- similarly for subgroups of G
- two subsets of G, A and B with $B = xAx^{-1}$ for some $x \in G$, said to be *conjugate*

Translation

Definition 31. [translation] *operation of G on itself defined by map*

$$(x, y) \mapsto xy$$

called translation*, denoted by* $T_x : G \to G$ *with* $T_x(y) = xy$

- for subgroup, $H \subset G$, $T_x(H) = xH$ is left coset
  - denote set of left cosets also by G/H even if H is not normal
  - denote set of right cosets also by $H\backslash G$
- examples of translation
  - $G = GL(V)$, group of linear automorphism of vector space with field, F, for which, map, $(A, v) \mapsto Av$ for $A \in G$ and $v \in V$, defines operation of G on V
    - G is subgroup of group of permutations, $\mathrm{Perm}(V)$
  - for $V = F^n$, G is group of nonsingular n-by-n matrices

Isotropy

Definition 32. [isotropy] *for operation of group, G, on set, S,*

$$\{x \in G | xs = s\}$$

called isotropy of G*, denoted by* G_s*, which is subgroup of* G

- for conjugation operation of group, G, G_s is normalizer of $s \in G$
- isotropy groups are conjugate, $e.g.$, for $s, s' \in S$ and $y \in G$ with $ys = s'$,

$$G_{s'} = yG_s y^{-1}$$

- by definition, kernel of operation of G on S is

$$K = \bigcap_{s \in S} G_s \subset G$$

- operation with trivial kernel, said to be *faithful*
- $s \in G$ with $G_s = G$, called *fixed point*

Orbits of operation

Definition 33. [orbits of operation] *for operation of group, G, on set, S, $\{xs|x \in G\}$, called* orbit of s under G*, denoted by* Gs

- for $x, y \in G$ in same coset of G_s, $xs = ys$, *i.e.* $(\exists z \in G)\,(x, y \in zG_s) \Leftrightarrow xs = ys$
- hence, mapping, $G/G_s \to S$, with $x \mapsto xG_s$, is morphism of G-sets, thus

Proposition 14. *for group, G, operating on set, S, and $s \in S$, order of orbit, Gs, is equal to index, $(G : G_s)$*

Proposition 15. *for subgroup, H, of group, G, number of conjugate subgroups to H is index of normalizer of H in G*

Definition 34. [transitive operation] *operation with one orbit, said to be* transitive

Orbit decomposition and class formula

- orbits are disjoint

$$S = \coprod_{\lambda \in \Lambda} G s_\lambda$$

  where s_λ are elements of distinct orbits

Formula 1. [orbit decomposition formula] *for group, G, operating on set, S, index set, Λ, whose elements represent distinct orbits*

$$|S| = \sum_{\lambda \in \Lambda} (G : G_\lambda)$$

Formula 2. [class formula] *for group, G, and set, $C \subset G$, whose elements represent distinct conjugacy classes*

$$(G : 1) = \sum_{x \in C} (G : G_x)$$

Sylow subgroups

Definition 35. [sylow subgroups] *for prime number, p, finite group with order, p^n for some $n \geq 0$, called p-group; subgroup $H \subset G$, of finite group, G, with order, p^n for some $n \geq 0$, called p-subgroup; subgroup of order, p^n, where p^n is highest power of p dividing order of G, called p-Sylow subgroup*

Lemma 2. *finite abelian group of order divided by prime number, p, has subgroup of order p*

Theorem 7. [p-Sylow subgroups of finite groups] *finite group of order divided by prime number, p, has p-Sylow subgroup*

Lemma 3. [number of fixed points of group operations] *for p-group, H, operating on finite set, S*

- *number of fixed points of H is congruent to size of S modulo p, $i.e.$*

$$\#\text{ fixed points of } H \equiv |S| \pmod{p}$$

- *if H has exaxctly one fixed point, $|S| = 1 \pmod{p}$*
- *if p divides $|S|$, $|S| = 0 \pmod{p}$*

Sylow subgroups and solvability

Theorem 8. [solvability of finite p-groups] *finite p-group is solvable; if it is non-trivial, it has non-trivial center*

Corollary 1. *for non-trivial p-group, exists sequence of subgroups*

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$$

where G_i is normal in G and G_{i+1}/G_i is cyclic group of order, p

Lemma 4. [normality of subgroups of order p] *for finite group, G, smallest prime number dividing order of G, p, every subgroup of index p is normal*

Proposition 16. *group of order, pq, with p and q being distinct prime numbers, is solvable*

- now can prove following
  - group of order, 35, is solvable - implied by Proposition 8 and Proposition 12
  - group of order less than 60 is solvable

Rings

Rings

Definition 36. [rings] *set, A, together with two laws of composition called multiplication and addition which are written as product and sum respectively, satisfying following conditions, called* ring

- *A is commutative group with respect to addition - unit element denoted by 0*
- *A is monoid with respect to multiplication - unit element denoted by 1*
- *multiplication is distributive over addition, $i.e.$*

$$(\forall x, y, z \in A)\,((x+y)z = xz + yz \;\&\; z(x+y) = zx + zy)$$

do not assume $1 \neq 0$

- can prove, $e.g.$,
  - $(\forall x \in A)\,(0x = 0) \because 0x + x = 0x + 1x = (0+1)x = 1x = x$
  - if $1 = 0$, $A = \{0\} \because x = 1x = 0x = 0$
  - $(\forall x, y \in A)\,((-x)y = -(xy)) \because xy + (-x)y = (x + -x)y = 0y = 0$
  - $(\forall x, y \in A)\,((-x)(-y) = xy) \because (-x)(-y) + (-(xy)) = (-x)(-y) + (-x)y = (-x)(-y+y) = (-x)0 = 0$

Kinds of rings

Definition 37. [groups of units of rings] *subset, U, of ring, A, such that every element of U has both left and right inverses, called* group of units of A *or* group of invertible elements of A*, sometimes denoted by* A^*

Definition 38. [division rings] *ring with $1 \neq 0$ and every nonzero element being invertible, called* division ring

Definition 39. [multiplicative groups of invertible elements of rings] *we denote multiplicative groups of invertible elements of rings, A, by* A^*

Definition 40. [commutative rings] *ring, A, with $(\forall x, y \in A)\,(xy = yx)$, called* commutative ring

Definition 41. [fields] *commutative division ring, called* field

Definition 42. [subrings] *subset of ring which itself is ring with same additive and multiplicative laws of composition, called* subring

Definition 43. [center of rings] *subset,* $C \subset A$*, of ring,* A *such that*

$$C = \{a \in A | \forall x \in A, xa = ax\}$$

is subring, *called* center of ring, A

General distributivity and ring examples

- general distributivity - for ring, A, $\langle x_i \rangle_{i=1}^n \subset A$, $\langle y_i \rangle_{i=1}^n \subset A$

$$\left(\sum x_i\right)\left(\sum y_j\right) = \sum_i \sum_j x_i y_j$$

- ring examples
  - for set, S, and ring, A, set of all mappings of S into A, $\mathrm{Map}(S, A)$ whose addition and multiplication are defined as below, is *ring*

$$(\forall f, g \in \mathrm{Map}(S, A), x \in S)\,((f + g)(x) = f(x) + g(x))$$

$$(\forall f, g \in \mathrm{Map}(S, A), x \in S)\,((fg)(x) = f(x)g(x))$$

    - additive and multiplicative unit elements of $\mathrm{Map}(S, A)$ are constant maps whose values are additive and multiplicative of A respectively
  - for abelian group, M, set, $\mathrm{End}(M)$ of group homeomorphisms of M into itself is ring with normal addition and mapping composition as multiplication, is *ring* - not commutative in general

Group rings and convolution products

Definition 44. [group rings] *for group, G, and field, K, set of all formal linear combinations, $\sum_{x\in G} a_x x$, with $a_x \in K$ where a_x are zero except finite number of them, where addition is defined normally and multiplication is defined as*

$$\left(\sum_{x\in G} a_x x\right)\left(\sum_{y\in G} b_y y\right) = \sum_{z\in G}\left(\sum_{xy=z} a_x b_y xy\right)$$

called group ring, *denoted by* $K[G]$, *and* $\sum_{xy=z} a_x b_y$, *called* convolution product

Ideals of rings

Definition 45. [ideals] *subset, $\mathfrak{a}$, of ring, A, which is subgroup of additive group of A, with $A\mathfrak{a} \subset \mathfrak{a}$, called* left ideal *- indeed, $A\mathfrak{a} = \mathfrak{a}$ because A has 1; right ideal can be similarly defined, $i.e.$, $\mathfrak{a}A = \mathfrak{a}$; subset which is both left and right ideal is* two-sided ideal

Definition 46. [principals] *for ring, A, and $a \in A$, left ideal, Aa, called* principal left ideal*; AaA, called* principal two-sided ideal

Definition 47. [generators of ideals] *for ring, A, and $a_1, \ldots, a_n$, set of elements of A of form*

$$\sum x_i a_i$$

with $x_i \in A$, is left ideal, and denoted by $(a_1, \ldots, a_n)$, called generators *of the left ideal; similarly for right ideals*

- above equal to smallest ideals containing a_i, $i.e.$, intersection of all ideals containing a_i $\bigcap_{a_1,\ldots,a_n \in \mathfrak{a}} \mathfrak{a}$ - just like set (σ-)algebras in set theory on page **??** (proof can be found in Proof 3)

Definition 48. [principal rings] *commutative ring of which every ideal is principal and* $1 \neq 0$, *called* principal ring

Ring homeomorphisms

Definition 49. [ring homeomorphisms] *mapping of ring into ring, $f : A \to B$, such that f is monoid-homeomorphism for both additive and multiplicative structure on A and B, $i.e.*

$$(a, b \in A)\,(f(a+b) = f(a) + f(b)\ \&\ f(ab) = f(a)f(b))$$

and

$$f(1) = 1\ \&\ f(0) = 0$$

called ring-homeomorphism*;* kernel*, defined to be kernel of f viewed as additive homeomorphism*

- *kernel of ring-homeomorphism, $f : A \to B$,* is ideal of A
- conversely, for ideal, $\mathfrak{a}$, can construct factor ring, $A/\mathfrak{a}$
- simply say "homeomorphism" if reference to rings is clear

Proposition 17. [injectivity of field homeomorphisms] *(ring) homeomorphism from field into field is injective*

Factor rings and canonical maps

Definition 50. [factor rings and residue classes] *for ring,* A, $\mathfrak{a}$, *set of cosets,* $x + \mathfrak{a}$ *for* $x \in A$, *combined with* addition *defined by viewing* A *and* $\mathfrak{a}$ *as additive groups,* multiplication *defined by*

$$(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a},$$

which satisfy all requirements for ring, called factor ring *or,* residue class ring, *denoted by* $A/\mathfrak{a}$; *cosets in* $A/\mathfrak{a}$, *called* residue classes modulo $\mathfrak{a}$, *and each coset,* $x + \mathfrak{a}$, *called* residue class of x modulo $\mathfrak{a}$

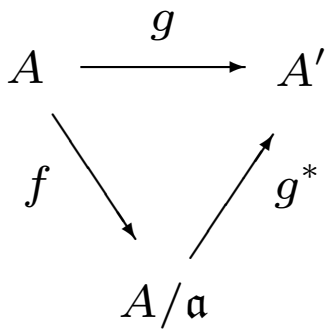
Definition 51. [canonical maps of rings] *ring-homeomorphism of ring,* A, *into factor ring,* $A\mathfrak{a}$

$$A \to A/\mathfrak{a}$$

called canonical map of A into $A/\mathfrak{a}$

Factor ring induced ring-homeomorphism

Proposition 18. [factor ring induced ring-homeomorphism] *for ring-homeomorphism, $f : A \to A'$ whose kernel contains ideal, $\mathfrak{a}$, exists unique ring-homeomorphism, $g_* : A/\mathfrak{a} \to A'$, making diagram in figure commutative*



- ring canonical map, $f : A \to A/\mathfrak{a}$, is universal in category of homeomorphisms whose kernel contains $\mathfrak{a}$

Embedding of rings

- bijective ring-homeomorphism, $f : A \to B$ is isomorphism
  - indeed, exists set-theoretic inverse, $g : B \to A$, of f, which is ring-homeomorphism
- image, $f(A)$, of ring-homeomorphism, $f : A \to B$, is subring of B

Definition 52. [embedding of rings] *ring-isomorphism between A and its image, established by injective ring-homeomorphism, $f : A \to B$, called* embedding of rings

Definition 53. [induced injective ring-homeomorphisms] *for ring-homeomorphism, $f : A \to A'$ and ideal $\mathfrak{a}'$ of A', injective ring-homeomorphism*

$$A/f^{-1}(\mathfrak{a}') \to A'/\mathfrak{a}'$$

called induced injective ring-homeomorphism

Zero divisors and entire rings

Definition 54. [zero divisors] *for ring,* A, $x, y \in A$ *with* $x \neq 0$, $y \neq 0$, $xy = 0$, *said to be* zero divisors

Definition 55. [entire rings] *commutative ring with no zero divisors for which* $1 \neq 0$, *said to be* entire*; entire rings sometimes called* integral domains

Ideals of commutative rings and fields

Definition 56. [prime ideals] *for commutative ring,* A*, ideal* $\mathfrak{p} \neq A$ *with* $A/\mathfrak{p}$ *entire, called* prime ideal *or just* ideal*; equivalently, ideal,* $\mathfrak{p} \neq A$ *is* prime if and only if

$$(\forall x, y \in A)\,(xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \text{ or } y \in \mathfrak{p})$$

Definition 57. [maximal ideals] *for commutative ring,* A*, ideal* $\mathfrak{m} \neq A$ *such that*

$$(\forall \text{ ideal } \mathfrak{a} \subset A)\,(\mathfrak{m} \subset \mathfrak{a} \Rightarrow \mathfrak{a} = A)$$

called maximal ideal

Lemma 5. [properties of prime and maximal ideals] *for commutative ring,* A

- *every maximal ideal is prime*
- *every ideal is contained in some maximal ideal*
- *ideal,* $\{0\}$ *is prime* if and only if A *is entire*
- *only ideals of field is either zero ideal or the field itself*
- *ideal,* $\mathfrak{m}$*, is maximal* if and only if $A/\mathfrak{m}$ *is field*
- *inverse image of prime ideal of commutative ring homeomorphism is prime*

Characteristic of rings

- consider ring-homeomorphism
$$\lambda : \mathbf{Z} \to A$$
for ring, A, such that
$$\lambda(n) = ne$$
where e is multiplicative unit element of A
  - kernel of λ is ideal (n), for $n \in \mathbf{Z}$, $i.e.$, ideal generated by integer, n
  - hence, canonical injective ring-homeomorphism, $\mathbf{Z}/n\mathbf{Z} \to A$, which is ring-isomorphism between $\mathbf{Z}/n\mathbf{Z} \to A$ and subring of A
  - when $n\mathbf{Z}$ is prime ideal, exist two cases; either $n = 0$ or $n = p$ for prime number, p

Definition 58. [characteristic of rings] *ring, A, with $\{0\}$ as prime ideal kernel above, said to have characteristic 0; if prime ideal kernel is $p\mathbf{Z}$ for prime number, p, A, said to have characteristic p, in which case, A contains (isomorphic image of) $\mathbf{Z}/p\mathbf{Z}$ as subring, abbreviated by $\mathbf{F}_p$*

Prime fields and prime rings

- field, K, has characteristic 0 or p for prime number, p

- K contains (isomorphic image of) $\mathbf{Q}$ or $\mathbf{F}_p$ for first and second cases respectively, as subfield

Definition 59. [prime fields and prime rings] *in above cases, both* $\mathbf{Q}$ *and* $\mathbf{F}_p$*, called* prime field (contained in K)*; since prime field is smallest subfield of* K *containing* 1 *having no automorphism other than identity, identify it with* $\mathbf{Q}$ *or* $\mathbf{F}_p$ *for each case;* prime ring (contained in K) *means either integers,* $\mathbf{Z}$*, if* K *has characteristic* 0*, or* $\mathbf{F}_p$ *if* K *has characteristic* p

$\mathbf{Z}/n\mathbf{Z}$

- **Z** is ring
- every ideal of **Z** is principal (proof can be found in Proof 4), $i.e.$, either $\{0\}$ or $n\mathbf{Z}$ for some $n \in \mathbf{N}$
- ideal of **Z** is prime *if and only if* is $p\mathbf{Z}$ for some prime number, $p \in \mathbf{N}$
  - $p\mathbf{Z}$ is maximal ideal

Definition 60. [rings of integers modulo n] $\mathbf{Z}/n\mathbf{Z}$, *called* ring of integers modulo n; *abbreviated as* mod n

- $\mathbf{Z}/p\mathbf{Z}$ for prime p is *field* and denoted by $\mathbf{F}_p$

Euler phi-function

Definition 61. [Euler phi-function] *for $n > 1$, order of divison ring of $\mathbf{Z}/n\mathbf{Z}$, calleds* Euler phi-function, *denoted by $\varphi(n)$; if prime factorization of n is*

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

with distinct prime numbers, p_i, and $e_i \geq 1$

$$\varphi(n) = p_1^{e_1-1}(p_1 - 1) \cdots p_r^{e_r-1}(p_r - 1)$$

Theorem 9. [Euler's theorem] *for x prime to n,*

$$x^{\varphi(n)} \equiv 1 \pmod{n}$$

Chinese remainder theorem

Theorem 10. [Chinese remainder theorem] *for ring,* A *and* $n \geq 2$ *ideals,* $\mathfrak{a}_1, \ldots \mathfrak{a}_n$ *with* $\mathfrak{a}_i + \mathfrak{a}_j = A$ *for all* $1 \leq i \neq j \leq n$

$$(\forall x_1, \ldots, x_n \in A)\,(\exists x \in A)\,(\forall 1 \leq i \leq n)\,(x \equiv x_i \pmod{\mathfrak{a}_i})$$

Corollary 2. [isomorphism induced by Chinese remainder theorem] *for ring,* A*,* $n \geq 2$ *ideals,* $\mathfrak{a}_1, \ldots \mathfrak{a}_n$ *with* $\mathfrak{a}_i + \mathfrak{a}_j = A$ *for all* $1 \leq i \neq j \leq n$*, and map of* A *into product induced by canonical map of* A *onto* $A/\mathfrak{a}_i$ *for each factor,* $i.e.$*,*

$$f : A \to \prod A/\mathfrak{a}_i$$

- f *is surjective,*
- $\operatorname{Ker} f = \bigcap \mathfrak{a}_i$,
- *hence, there is isomorphism*

$$A/\cap \mathfrak{a}_i \approx \prod A/\mathfrak{a}_i$$

Isomorphisms of endomorphisms of cyclic groups

Theorem 11. [isomorphisms of endomorphisms of cyclic groups] *for cyclic group, A, of order, n, endomorphisms of A into A, with, $x \mapsto kx$, for $k \in \mathbf{Z}$ induce*

- *ring isomorphism*

$$\mathbf{Z}/n\mathbf{Z} \approx \mathrm{End}(A)$$

and

- *group isomorphism*

$$(\mathbf{Z}/n\mathbf{Z})^* \approx \mathrm{Aut}(A)$$

where B^* denotes multiplicative groups of invertible elements of ring, B, as defined in Definition 39

- $e.g.$, for group of n-th roots of unity in $\mathbf{C}$, μ_n, all automorphisms are given by

$$\xi \mapsto \xi^k$$

for $k \in (\mathbf{Z}/n\mathbf{Z})^*$

Irreducibility and factorial rings

Definition 62. [irreducible ring elements] *for entire ring, A, non-unit non-zero element, $a \in A$, with*

$$(\forall b, c \in A)\,(a = bc \Rightarrow b \text{ or } c \text{ is unit})$$

said to be irreducible

Definition 63. [unique factorization into irreducible elements] *for entire ring, A, element, $a \in A$, for which exists unit, u, and irreducible elements, $p_1, \ldots, p_r$ in A such that*

$$a = u \prod p_i$$

and this expression is unique up to permutation and multiplications by units, said to have unique factorization into irreducible elements

Definition 64. [factorial rings] *entire ring with every non-zero element has unique factorial into irreducible elements, called* factorial ring *or* unique factorization ring

Devision and greatest common divisor (g.c.d.)

Definition 65. [devision of entire ring elements] *for entire ring, A, and nonzero elements, $a, b \in A$, if exists $c \in A$ such that $ac = b$, we say a divides b, denoted by $a|b$*

Definition 66. [greatest common divisor (g.c.d.)] *for entire ring, A, and $a, b \in A$, $d \in A$ which divides a and b and satisfies*

$$(\forall c \in A \text{ with } c|a \ \& \ c|b)\ (c|d)$$

called greatest common divisor (g.c.d.) of a and b

Proposition 19. [existence of greatest common divisor of principal entire rings] *for principal entire ring, A, and nonzero $a, b \in A$, $c \in A$ with $(a, b) = (c)$ is g.c.d. of a and b*

Theorem 12. [principal entire ring is factorial] *principal entire ring is factorial*

Polynomials

Why (rings of) polynomials?

- lays ground work for polynomials in general

- needs polynomials over arbitrary rings for diverse purposes
  - polynomials over finite field which cannot be identified with polynomial functions in that field
  - polynomials with integer coefficients; reduce them mod p for prime, p
  - polynomials over arbitrary commutative rings
  - rings of polynomial differential operators for algebraic geometry & analysis

Defintion of polynomials

- exist many ways to define polynomials over commutative ring
- here's one

Definition 67. [polynomials] *for ring, A, infinite cyclic group generated by X, and monoid $S = \{X^r | r \in \mathbf{Z}, r \geq 0\}$, set of functions from S into A which are equal to 0 except finite number of elements of S, called* polynomials over A*, denoted by* $A[X]$

- for every $a \in A$, define function which has value, a, on X^n, and value, 0, for every other element of S, by aX^r
- then, *a* polynomial can be uniquely written as

$$f(X) = a_0X^0 + \cdots + a_nX^n$$

  for some nonnegative $n \in \mathbf{Z}$, $a_i \in A$
- a_i, called *coefficients of f*

Polynomial functions

Definition 68. [polynomial functions] *for two rings, A and B, with $A \subset B$, and $f \in A[X]$ with $f(X) = a_0 + a_1X + \cdots + a_nX^n$, map, $f_B : B \to B$ defined by*

$$f_B(x) = a_0 + a_1x + \cdots + a_nx^n$$

called polynomial function associated with $f(X)$

Definition 69. [evaluation homeomorphism] *for two rings, A and B, with $A \subset B$, and $b \in B$, ring homeomorphism from $A[X]$ into B with association, $\mathrm{ev}_b : f \mapsto f(b)$, called* evaluation homeomorphism, *said to be obtained by* substituting b for X in f

- hence, for $x \in B$, subring, $A[x]$ of B generated by x over A is ring of all polynomial values, $f(x)$, for $f \in A[X]$

Definition 70. [variables and transcendentality] *for two rings, A and B, with $A \subset B$, if x makes evaluation homeomorphism, $\mathrm{ev}_x : f \mapsto f(x)$, isomorphic, x, said to be* transcendental over A *or* variable over A

- in particular, X *is variable over* A

Polynomial examples

- consider $\alpha = \sqrt{2}$ and $\{a + b\alpha \,|a, b \in \mathbf{Z}\}$, subring of $\mathbf{Z}[\alpha] \subset \mathbf{R}$ generated by α.
  - α is *not* transcendental because $f(\alpha) = 0$ for $f(X) = X^2 - 1$, hence kernel of evaluation map of $\mathbf{Z}[X]$ into $\mathbf{Z}[\alpha]$ is not injective, hence not isomorphism

- consider $\mathbf{F}_p$ for prime number, p
  - $f(X) = X^p - X \in \mathbf{F}_p[X]$ is not zero polynomial, but because $x^{p-1} \equiv 1$ for every x prime to p by Theorem 9 (Euler's theorem), hence $x^p \equiv x$ for every $x \in \mathbf{F}_p$, thus for polynomial function, $f_{\mathbf{F}_p}$, $f_{\mathbf{F}_p}(x) = 0$ for every x in $\mathbf{F}_p$
  - $i.e.$, non-zero polynomial induces zero polynomial function

Reduction map

- for homeomorphism, $\varphi : A \to B$, of commutative rings, exists associated homeomorphisms of polynomials rings, $A[X] \to B[X]$, such that

$$f(X) = \sum a_i X^i \mapsto \sum \varphi(a_i) X^i = (\varphi f)(X)$$

Definition 71. [reduction maps] *above ring homeomorphism, $f \mapsto \varphi f$, called* reduction map

- $e.g.$, for complex conjugate, $\varphi : \mathbf{C} \to \mathbf{C}$, homeomorphism of $\mathbf{C}[X]$ into itself can be obtained by reduction map, $f \mapsto \varphi f$, which is complex conjugate of polynomials with complex coefficients

Definition 72. [reduction of f modulo p] *for prime ideal, $\mathfrak{p}$, of ring, A, surjective canonical map, $\varphi : A \to A/\mathfrak{p}$, reduction map, φf for $f \in A[X]$, sometimes called* reduction of f modulo p

Basic properties of polynomials in one variable

Theorem 13. [Euclidean algorithm] *for set of all polynomials in one variable of nonnegative degrees, $A[X]$, with commutative ring, A*

$$(\forall f, g \in A[X] \text{ with leading coefficients of } g \text{ unit in } A)$$
$$(\exists q, r \in A[X] \text{ with } \deg r < \deg g)\,(f = qg + r)$$

Theorem 14. [principality of polynomial rings] *polynomial ring in one variable, $k[X]$, with field, k, is principal*

Constant, monic, and irreducible polynomials

Definition 73. [constant and monic polynomials] $k \in k[X]$, *with field,* k, *called* constant polynomial; $f(x) \in k[X]$ *with leading coefficient,* 1, *called* monic polynomial

Definition 74. [irreducible polynomials] *polynomial* $f(x) \in k[X]$ *such that*

$$(\forall g(X), h(X) \in k[X])\,(f(X) = g(X)h(X) \Rightarrow g(X) \in k \text{ or } h(X) \in k)$$

said to be irreducible

Root or zero of polynomials

Definition 75. [roots] *for commutator ring, B, its subring, $A \subset B$, and $f(x) \in A[X]$ in one variable, $b \in B$ satisfying*

$$f(b) = 0$$

called root *or* zero *of f;*

Theorem 15. [roots of polynomials] *for field, k, polynomial, $f \in k[X]$ in one variable of degree, $n \geq 0$, has at most n roots in k; if a is root of f in k, $X - a$ divides $f(X)$*

Induction of zero functions

Corollary 3. [induction of zero functions in one variable] *for field, k, infinite subset, $T \subset k$, if polynomial, $f \in k[X]$, in one variable over k, satisfies*

$$(\forall a \in k)\,(f(a) = 0)$$

then $f(0) = 0$, $i.e.$, f induces zero function

Corollary 4. [induction of zero functions in multiple variables] *for field, k, and n infinite subsets of k, $\langle S_i \rangle_{i=1}^{n}$, if polynomial in n variables over field, k, satisfies*

$$(\forall a_i \in S_i \text{ for } 1 \leq i \leq n)\,(f(a_1, \ldots, a_n) = 0)$$

then $f = 0$, $i.e.$, f induces zero function

Corollary 5. [induction of zero functions in multiple variables - infinite fields] *if polynomial in n variables over infinite field, k, induces zero function in $k^{(n)}$, $f = 0$*

Corollary 6. [induction of zero functions in multiple variables - finite fields] *if polynomial in n variables over finite field, k, of order, q, degree of which in each variable is less than q, induces zero function in $k^{(n)}$, $f = 0$*

Reduced polynomials and uniqueness

- for field, k, with q elements, polynomial in n variables over k can be expressed as

$$f(X_1, \ldots, X_n) = \sum a_i X_1^{\nu_{i,1}} \cdots X_n^{\nu_{i,n}}$$

  for finite sequence, $\langle a_i \rangle_{i=1}^{m}$, and $\langle \nu_{1,j} \rangle_{j=1}^{n}$, $\ldots$, $\langle \nu_{m,j} \rangle_{j=1}^{n}$ where $a_i \in k$ and $\nu_{i,j} \geq 0 \in \mathbf{Z}$
- for each $\nu_{i,j}$, exist $g_{i,j} \geq 0$ and $0 \leq r_{i,j} < q$ such that $\nu_{i,j} = g_{i,j}q + r_{i,j}$ (by Euclidean algorithm), thus f can be rewritten as

$$f(X_1, \ldots, X_n) = \sum a_i X_1^{r_{i,1}} \cdots X_n^{r_{i,n}}$$

  because $X_i^q = 1$
- called *reduced polynomial*, denoted by f^*

Corollary 7. [uniqueness of reduced polynomials] *for field, k, with q elements, reduced polynomial is unique (by Corollary 6)*

Multiplicative subgroups and n-th roots of unity

Definition 76. [multiplicative subgroups of fields] *for field, k, subgroup of group, $k^* = k \sim \{0\}$, called* multiplicative subgroup of k

Theorem 16. [finite multiplicative subgroups of field is cyclic] *finite multiplicative subgroup of field, k, is cyclic*

Corollary 8. [multiplicative subgroup of finite field is cyclic] *multiplicative subgroup of finite field is cyclic*

Definition 77. [primitive n-th roots of unity] *generator for group of n-th roots of unity, called* primitive n-th root of unity*; group of roots of unity, denoted by μ; group of roots of unity in field, k, denoted by $\mu(k)$*

Algebraic closedness

Definition 78. [algebraically closed] *field, k, for which every polynomial in $k[X]$ of positive degree has root in k, said to be* algebraically closed

- $e.g.$, complex numbers are algebraically closed
- every field is contained in some algebraically closed field
- for algebraically closed field, k
  - every irreducible polynomial in $k[X]$ is of degree 1
  - unique factorization of polynomial of nonnegative degree can be written in form

$$f(X) = c\prod_{i=1}^{r}(X-\alpha_i)^{m_i}$$

with $c \neq 0 \in k$ and distinct roots, $\alpha_1, \ldots, \alpha_r$

Derivatives of polynomials

Definition 79. [derivatives of polynomials over commutative rings] *for polynomial* $f(X) = a_n X^n + \cdots + a_0 \in A[X]$ *with commutative ring,* A*, where* $a_i \in A$*, map,* $D : A[X] \to A[X]$ *defined by*

$$Df(X) = na_n X^{n-1} + \cdots + a_1$$

called derivative of polynomial*, denoted by* $f'(X)$*;*

- for $f, g \in A[X]$ with commutative ring, A, and $a \in A$

$$(f+g)' = f' + g' \ \& \ (fg)' = f'g + fg' \ \& \ (af) = af'$$

Multiple roots and multiplicity

Definition 80. [multiplicity and multiple roots] *nonzero polynomial, $f(X) \in k[X]$, in one variable over field, k, having $a \in k$ as root can be written of form*

$$f(X) = (X - a)^m g(X)$$

with some polynomial, $g(X) \in A[X]$ relatively prime to $(X - a)$ (hence, $g(a) \neq 0$); m here, called multiplicity of a in f*, when $m > 1$, a, said to be* multiple root of f

Proposition 20. [necessary and sufficient condition for multiple roots] *for polynomial, f, of one variable over field, k, $a \in k$ is multiple root of f* if and only if *is root of f and $f'(a) = 0$*

Proposition 21. [derivatives of polynomials] *for polynomial, $f \in K[X]$ over field, K, of positive degree, $f' \neq 0$ if K has characteristic 0; if K has characteristic $p > 0$,* $f' = 0$ if and only if

$$f(X) = \sum_{\nu=1}^{n} a_\nu X^\nu$$

where p divides each integer, ν, with $a_\nu \neq 0$

Fields having characteristic p

- for prime, p, $p|\binom{p}{\nu}$ for all $1 \leq \nu < p$, hence for field, K, having characteristic p, and $a, b \in K$,
$$(a+b)^p = a^p + b^p$$
- applying this resurvely r times yields
$$(a+b)^{p^r} = (a^p + b^p)^{p^{r-1}} = (a^p + b^p)^{p^{r-2}} = \cdots = a^{p^r} + b^{p^r}$$
- thus, $(X-a)^{p^r} = X^{p^r} - a^{p^r}$
- if $c \in K$ and polynomial
$$X^{p^r} - c$$
has root $a \in K$, then $a^{p^r} = c$ and
$$X^{p^r} - c = (X-a)^{p^r}$$
- thus, has precisely one root, a, of multiplicity, p^r!

Frobenius endomorphisms

- homeomorphism of K into itself, $x \mapsto x^p$, has trivial kernel, hence injective

- hence, iterating $r \geq 1$ times yields endomorphism, $x \mapsto x^{p^r}$

Definition 81. [Frobenius endomorphisms] *for field, K, prime number, p, and $r \geq 1$, endomorphism of K into itself, $x \mapsto x^{p^r}$, called* Frobenius endomorphism

Algebraic Extensions

Algebraic extensions

- will show that for polynomial over field, always exists some extension of the field where the polynomial has root

- will show existence of algebraic closure for every field

Extensions of fields

Definition 82. [extensions of fields] *for field, E, and subfield, $F \subset E$, E said to be* extension field of F,

- *can view E vector space over F*
- *if dimension of the vector space is finite, the extension called* finite extension of F
- *if infinite, called* infinite extension of F

- extension, $F \subset E$, sometimes denoted by E/F, which should *not* confused with *factor group*, only when unambiguously understood

Algebraic over fields

Definition 83. [algebraic over fields] *for field, E, and subfield, $F \subset E$, $\alpha \in E$ with*

$$(\exists a_0, \ldots, a_n \ (n \geq 1) \text{ with not all } a_i \text{ zero}) \ (a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0)$$

said to be algebraic over F

- *for algebraic $\alpha \neq 0$, can always find such equation like above that $a_0 \neq 0$*

- equivalent statement to Definition 83
  - for field, E, and subfield, $F \subset E$, $\alpha \in E$ is algebraic over F *if and only if* exists homeomorphism, $\varphi : F[X] \to E$ such that

$$(\forall x \in F) \ (\varphi(x) = x) \ \ \& \ \varphi(X) = \alpha \ \& \ \operatorname{Ker} \varphi \neq \{0\}$$

- in which case, $\mathrm{Ker}\,\varphi$ is principal ideal (by Theorem 14), hence generated by single element, thus exists nonzero $p(X) \in F[X]$ (with normalized leading coefficient being 1) so that

$$F[X]/(p(X)) \approx F(\alpha)$$

- $F(\alpha)$ entire, hence $p(X)$ irreducible (refer to Definition 56)

Definition 84. [THE irreducible polynomial] *normalized $p(X)$ (i.e., with leading coefficient being 1) uniquely determined by α, called* THE irreducible polynomial of α over F, *denoted by* $\mathrm{Irr}(\alpha, F, X)$

Algebraic extensions

Definition 85. [algebraic extensions] *for field, F, its extension field, every element of which is algebraic over F, said to be* algebraic extension of F

Proposition 22. [algebraic-ness of finite field extensions] *every finite extension field of field, F, is algebraic over F*

- converse is *not* true, $e.g.$, subfield of complex numbers consisting of algebraic numbers over $\mathbf{Q}$ is infinite extension of $\mathbf{Q}$

Dimension of extensions

Definition 86. [dimension of extensions] *for field, F, dimension of its extension, E, as vector space over F, called* dimension of E over F, *denoted by* $[E : F]$

Proposition 23. [dimension of finite extensions] *for field, k, and its extension fields, F and E, with $k \subset F \subset E$,*

$$[E : k] = [E : F][F : k]$$

- *if $\langle x_i \rangle_{i \in I}$ is basis for F over k, and $\langle y_j \rangle_{j \in J}$ is basis for E over F, $\langle x_i y_j \rangle_{(i,j) \in I \times J}$ is basis for E over k*

Corollary 9. [finite dimensions of extensions] *for field, k, and its extension fields, F and E, with $k \subset F \subset E$, extension of E over k is finite* if and only if *extension of F over k is finite and extension of E over F is finite*

Generation of field extensions

Definition 87. [generation of field extensions] *for field, k, its extension field, E, and $\alpha_1, \ldots, \alpha_n \in E$, smallest subfield containing k and $\alpha_1, \ldots, \alpha_n$, said to be* finitely generated over k by $\alpha_1, \ldots, \alpha_n$, *denoted by* $k(\alpha_1, \ldots, \alpha_n)$

- $k(\alpha_1, \ldots, \alpha_n)$ consists of all quotients, $f(\alpha_1, \ldots, \alpha_n)/g(\alpha_1, \ldots, \alpha_n)$ where $f, g \in k[X]$ and $g(\alpha_1, \ldots, \alpha_n) \neq 0$, *i.e.*

$$\begin{aligned} & k(\alpha_1, \ldots, \alpha_n) \\ = \quad & \{f(\alpha_1, \ldots, \alpha_n)/g(\alpha_1, \ldots, \alpha_n) \,|\, f, g \in f[X], g(\alpha_1, \ldots, \alpha_n) \neq 0\} \end{aligned}$$

- *any* field extension, $k \subset E$, is union of smallest subfields containing $\alpha_1, \ldots, \alpha_n$ where $\alpha_1, \ldots, \alpha_n$ range over finite set of elements of E, *i.e.*

$$E = \bigcup_{n \in \mathbf{N}} \bigcup_{\alpha_1, \ldots, \alpha_n \in E} k(\alpha_1, \ldots, \alpha_n)$$

Proposition 24. [finite extension is finitely generated] *every finite extension of field is finitely generated*

Tower of fields

Definition 88. [tower of fields] *sequence of extension fields*

$$F_1 \subset F_2 \subset \cdots \subset F_n$$

called tower of fields

Definition 89. [finite tower of fields] *tower of fields, said to be* finite if and only if *each step of extensions is finite*

Algebraic-ness of finitely generated subfields

Proposition 25. [algebraic-ness of finitely generated subfields by single element] *for field, k and $\alpha \in k$ being algebraic over k,*

$$k(\alpha) = k[\alpha]$$

and

$$[k(\alpha) : k] = \deg \mathrm{Irr}(\alpha, k, X)$$

hence $k(\alpha)$ is finite extension of k, thus algebraic extension over k *(by Proposition 22)*

Lemma 6. [a fortiori algebraic-ness] *for field, k, its extension, F, and α being algebraic over k where $k(\alpha)$ and F are subfields of common field, α is algebraic over F*

- *indeed,* $\mathrm{Irr}(\alpha, k, X)$ *has* a fortiori *coefficients in F*

- assume tower of fields

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \ldots, \alpha_n)$$

where α_i is algebraic over k

- then, α_{i+1} is algebraic over $k(\alpha_1, \ldots, \alpha_i)$ (by Lemma 6)

Proposition 26. [algebraic-ness of finitely generated subfields by multiple elements] *for field, k, and $\alpha_1, \ldots, \alpha_n$ being algebraic over k, $E = k(\alpha_1, \ldots, \alpha_n)$ is finitely algebraic over k (because of Proposition 25, Corollary 9, and Proposition 22). Indeed, $E = k[\alpha_1, \ldots, \alpha_n]$ and*

$$\begin{aligned}&[k(\alpha_1, \ldots, \alpha_n) : k] \\ &\quad = \quad \mathrm{Irr}(\alpha_1, k, X)\,\mathrm{Irr}(\alpha_2, k(\alpha_1), X) \cdots \mathrm{Irr}(\alpha_n, k(\alpha_1, \ldots, \alpha_{n-1}), X)\end{aligned}$$

(proof can be found in Proof 5)

Compositum of subfields and lifting

Definition 90. [compositum of subfields] *for field, k, its extensions, E and F, which are subfields of common field, L, smallest subfield of L containing both E and F, called* compositum of E and F in L, *denoted by* EF

- *cannot define compositum if E and F are not embedded in common field, L*

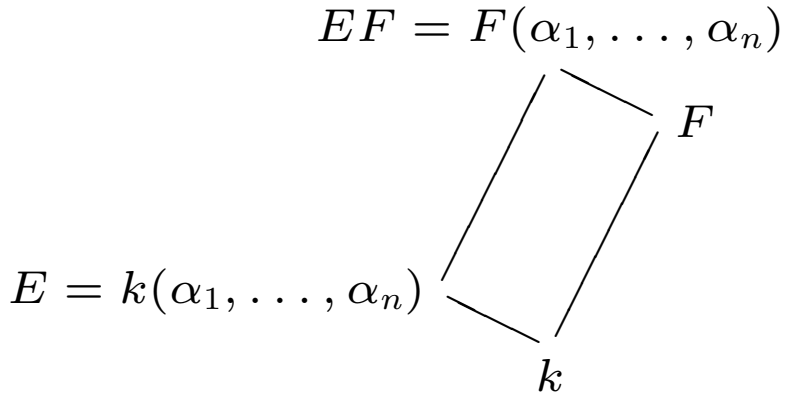
- could define *compositum of set of subfields of L* as smallest subfield containing subfields in the set
- extension, E, of k is compositum of all its finitely generated subfields over k, $i.e.$, $E = \bigcup_{n \in \mathbf{N}} \bigcup_{\alpha_1, \ldots, \alpha_n \in E} k(\alpha_1, \ldots, \alpha_n)$

Lemma 7. [finite generation of compositum] *for field, k, $E = k(\alpha_1, \ldots, \alpha_n)$, and F, any extension of k where both E and F are contained in common field, L,*

$$EF = F(\alpha_1, \ldots, \alpha_n),$$

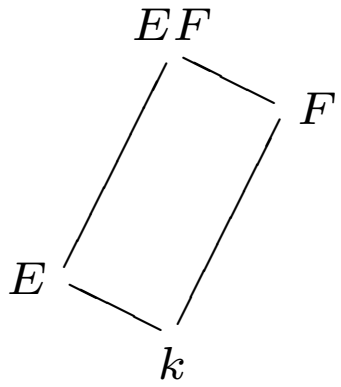
$i.e.$, compositum, EF, is finitely generated over F (proof can be found in Proof 6)

- *refer to diagra in figure*



Definition 91. [lifting] *extension, EF, of F, called* translation of E to F *or* lifting of E to F

- *often draw diagram as in figure*

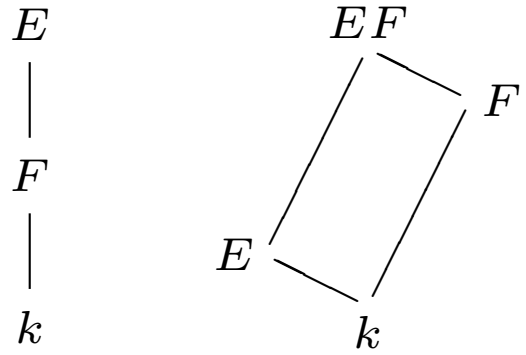


Distinguished classes

Definition 92. [distinguished class of field extensions] *for field, k, and its extension, E, class, $\mathcal{C}$, of extension fields satisfying*

- *for tower of fields, $k \subset F \subset E$, extension $k \subset E$ is in $\mathcal{C}$* if and only if *both $k \subset F$ and $F \subset E$ are in $\mathcal{C}$*
- *if $k \subset E$ is in $\mathcal{C}$, F is any extension of k, and both E and F are subfields of common field, then $F \subset EF$ is in $\mathcal{C}$*
- *if $k \subset F$ and $k \subset E$ are in $\mathcal{C}$ and both E and F are subfields of common field, $k \subset EF$ is in $\mathcal{C}$*

said to be distinguished*; figure illustrates first two properties - last property follows formally from first two properties*



Both algebraic and finite extensions are distinguished

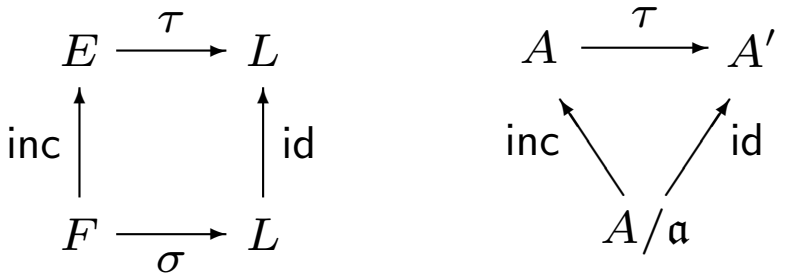
Proposition 27. [algebraic and finite extensions are distinguished] *class of algebraic extensions is distinguished, so is class of finite extensions*

- true that finitely generated extensions form distinguished class (not necessarily algebraic extensions or finite extensions)

Field embedding and embedding extensions

Definition 93. [field embedding] *for two fields, F and L, injective homeomorphism $\sigma : F \to L$, called* embedding of F into L*; then σ induces isomorphism of F with its image σF, which is sometimes written as F^σ*

Definition 94. [field embedding extensions] *for field embedding, $\sigma : F \to L$, field extension, $F \subset E$, and embedding, $\tau : E \to L$, whose restriction to F being equal to σ, said to* be over σ *or* extend σ*; if σ is identity, embedding, τ, called* embedding of E over F*; diagrams in figure show these embedding extensions*



- assuming same as in Definition 94, if $\alpha \in E$ is root of $f \in F[X]$, then α^τ is root of f^σ for if $f(X) = \sum_{i=0}^n a_i X^i$, then $f(\alpha) = \sum_{i=0}^n a_i \alpha^i = 0$, and $0 = f(\alpha)^\tau = \sum_{i=0}^n (a_i^\tau)(\alpha^\tau)^i = \sum_{i=0}^n a_i^\sigma (\alpha^\tau)^i = f^\sigma(\alpha^\tau)$

Embedding of field extensions

Lemma 8. [field embeddings of algebraic extensions] *for field, k, and its algebraic extension, E, embedding of E into itself over k is isomorphism*

Lemma 9. [compositums of fields] *for field, k, and its extensions, E and F, contained in common field,*

$$E[F] = F[E] = \bigcup_{n=1}^{\infty} \{e_1 f_1 + \cdots + e_n f_n \,|e_i \in E, f_i \in F\}$$

and EF is field of quotients of these elements

Lemma 10. [embeddings of compositum of fields] *for field, k, its extensions, E_1 and E_2, contained in commen field, E, and embedding $\sigma : E \to L$ for some field, L,*

$$\sigma(E_1 E_2) = \sigma(E_1)\sigma(E_2)$$

Existence of roots of irreducible polynomials

- assume $p(X) \in k[X]$ irreducible polynomial and consider canonical map, which is ring homeomorphism
$$\sigma : k[X] \to k[X]/((p(X))$$
- consider $\mathrm{Ker}\,\sigma|k$
  - every kernel of ring homeomorphism is ideal, hence if $a \neq 0 \in \mathrm{Ker}\,\sigma|k$, $1 \in \mathrm{Ker}\,\sigma|k$ because $a^{-1} \in \mathrm{Ker}\,\sigma|k$, but $1 \notin (p(X))$
  - thus, $\mathrm{Ker}\,\sigma|k = \{0\}$, hence $p^\sigma \neq 0$
- now for $\alpha = X^\sigma$
$$p^\sigma(\alpha) = p^\sigma(X^\sigma) = (p(X))^\sigma = 0$$
- thus, α is algebraic in k^σ, *i.e.*, $\alpha \in k[X]^\sigma$ is root of p^σ in $k^\sigma(\alpha)$

Lemma 11. [existence of root of irreducible polynomials] *for field, k, and irreducible $p(X) \in k[X]$ with $\deg p \geq 1$, exists homeomorphism of k, $\sigma : k \to L$, such that p^σ with $\deg p^\sigma \geq 1$ has root in field extension of k^σ*

Existence of algebraically closed algebraic field extensions

Proposition 28. [existence of extension fields containing roots] *for field, k, and $f \in k[X]$ with $\deg f \geq 1$, exists extension of k in which f has root*

Corollary 10. [existence of extension fields containing roots] *for field, k, and $f_1, \ldots, f_n \in k[X]$ with $\deg f_i \geq 1$, exists extension of k in which every f_i has root*

Definition 95. [algebraic closedness] *field, L, for which every polynomial, $f \in L[X]$ with $\deg f \geq 1$ has root in L, said to be* algebraically closed

Theorem 17. [existence of algebraically closed field extensions] *for field, k, exists algebraically closed extension*

Corollary 11. [existence of algebraically closed algebraic field extensions] *for field, k, exists algebraically closed algebraic extension of k (proof can be found in Proof 7)*

Isomorphism between algebraically closed algebraic extensions

Proposition 29. [number of algebraic embedding extensions] *for field, k, α being algebraic over k, algebraically closed field, L, and embedding, $\sigma : k \to L$, # possible embedding extensions of σ to $k(\alpha)$ in L is equal to # distinct roots of $\mathrm{Irr}(\alpha, k, X)$, hence no greater than # roots of $\mathrm{Irr}(\alpha, k, X)$*

Theorem 18. [algebraic embedding extensions] *for field, k, its algebraic extensions, E, algebraically closed field, L, and embedding, $\sigma : k \to L$, exists embedding extension of σ to E in L; if E is algebraically closed and L is algebraic over k^σ, every such embedding extension is isomorphism of E onto L*

Corollary 12. [isomorphism between algebraically closed algebraic extensions] *for field, k, and its algebraically closed algebraic extensions, E and E', exists isomorphism bewteen E and E' which induces identity on k, $i.e.$*

$$\tau : E \to E'$$

where $\tau|k$ is identity

- thus, *algebraically closed algebraic extension is determined up to isomorphism*

Algebraic closure

Definition 96. [algebraic closure] *for field, k, algebraically closed algebraic extension of k, which is determined up to isomorphism, called* algebraic closure of k*, frequently denoted by* k^{a}

- examples
  - complex conjugation is automorphism of $\mathbf{C}$ (which is the only continuous automorphism of $\mathbf{C}$)
  - subfield of $\mathbf{C}$ consisting of all numbers which are algebraic over $\mathbf{Q}$ is algebraic closure of $\mathbf{Q}$, *i.e.*, $\mathbf{Q}^{\mathrm{a}}$
  - $\mathbf{Q}^{\mathrm{a}} \neq \mathbf{C}$
  - $\mathbf{R}^{\mathrm{a}} = \mathbf{C}$
  - $\mathbf{Q}^{\mathrm{a}}$ *is countable*

Theorem 19. [countability of algebraic closure of finite fields] *algebraic closure of finite field is countable*

Theorem 20. [cardinality of algebraic extensions of infinite fields] *for infinite field, k, every algebraic extension of k has same cardinality as k*

Splitting fields

Definition 97. [splitting fields] *for field, k, and $f \in k[X]$ with $\deg f \geq 1$, field extension, K, of k, f splits into linear factors in which, $i.e.$,*

$$f(X) = c(X - \alpha_1) \cdots (X - \alpha_n)$$

and which is finitely generated over k by $\alpha_1, \ldots, \alpha_n$ (hence $K = k(\alpha_1, \ldots, \alpha_n)$), called splitting field of f

- for field, k, every $f \in k[X]$ has splitting field in k^{a}

Theorem 21. [isomorphism between splitting fields] *for field, k, $f \in k[X]$ with $\deg f \geq 1$, and two splitting fields of f, K and E, exists isomorphism between K and E; if $k \subset K \subset k^{\mathrm{a}}$, every embedding of E into k^{a} over k is isomorphism of E onto K*

Splitting fields for family of polynomials

Definition 98. [splitting fields for family of polynomials] *for field, k, index set, Λ, and indexed family of polynomials, $\{f_\lambda \in k[X] | \lambda \in \Lambda, \deg f_\lambda \geq 1\}$, extension field of k, every f_λ splits into linear factors in which and which is generated by all roots of all polynomials, f_λ, called* splitting field for family of polynomials

- in most applications, deal with finite Λ
- becoming increasingly important to consider infinite algebraic extensions
- various proofs would not be simpler if restricted ourselves to finite cases

Corollary 13. [isomorphism between splitting fields for family of polynomials] *for field, k, index set, Λ, and two splitting fields, K and E, for family of polynomials, $\{f_\lambda \in k[X] | \lambda \in \Lambda, \deg f_\lambda \geq 1\}$, every embedding of E into K^{a} over k is isomorphism of E onto K*

Normal extensions

Theorem 22. [normal extensions] *for field, k, and its algebraic extension, K, with $k \subset K \subset k^{\mathrm{a}}$, following statements are equivalent*

- *every embedding of K into k^{a} over k induces automorphism*
- *K is splitting field of family of polynomials in $k[X]$*
- *every irreducible polynomial of $k[X]$ which has root in K splits into linear factors in K*

Definition 99. [normal extensions] *for field, k, and its algebraic extension, K, with $k \subset K \subset k^{\mathrm{a}}$, satisfying properties in Theorem 22, said to be* normal

- *not* true that class of normal extensions is *distinguished*
  - $e.g.$, below tower of fields is tower of normal extensions

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt[4]{2})$$

  - but, extension $\mathbf{Q} \subset \mathbf{Q}(\sqrt[4]{2})$ is not normal because complex roots of $X^4 - 2$ are not in $\mathbf{Q}(\sqrt[4]{2})$

Retention of normality of extensions

Theorem 23. [retention of normality of extensions] *normal extensions remain normal under lifting; if $k \subset E \subset K$ and K is normal over k, K is normal over E; if K_1 and K_2 are normal over k and are contained in common field, K_1K_2 is normal over k, and so is $K_1 \cap K_2$*

Separable degree of field extensions

- for field, F, and its algebraic extension, E
  - let L be algebraically closed field and assume embedding, $\sigma : F \to L$
    - exists embedding extension of σ to E in L by Theorem 18
    - such σ maps E on subfield of L which is algebraic over F^σ
    - hence, E^σ is contained in algebraic closure of F^σ which is contained in L
    - will *assume* that L is the algebraic closure of F^σ
  - let L' be another algebraically closed field and assume another embedding, $\tau : F \to L'$ - assume as before that L' is algebraic closure of F^τ
  - then Theorem 18 implies, exists isomorphism, $\lambda : L \to L'$ extending $\tau \circ \sigma^{-1}$ applied to F^σ
  - let S_σ & S_τ be sets of embedding extensions of σ to E in L and L' respectively
  - then λ induces map from S_σ into S_τ with $\tilde{\sigma} \mapsto \lambda \circ \tilde{\sigma}$ and λ^{-1} induces inverse map from S_τ into S_σ, hence exists bijection between S_σ and S_τ, hence have same cardinality

Definition 100. [separable degree of field extensions] *above cardinality only depends on extension E/F, called* separable degree of E over F, *denoted by* $[E : F]_s$

Multiplicativity of and upper bound on separable degree of field extensions

Theorem 24. [multiplicativity of separable degree of field extensions] *for tower of algebraic field extensions,* $k \subset F \subset E$,

$$[E : k]_s = [E : F]_s [F : k]_s$$

Theorem 25. [upper limit on separable degree of field extensions] *for finite algebraic field extension,* $k \subset E$

$$[E : k]_s \leq [E : k]$$

- $i.e.$, separable degree is at most equal to degree ($i.e.$, dimension) of field extension

Corollary 14. *for tower of algebraic field extensions,* $k \subset F \subset E$, *with* $[E : k] < \infty$

$$[E : k]_s = [E : k]$$

holds if and only if *corresponding equality holds in every step of tower,* $i.e.$, *for* E/F *and* F/k

Finite separable field extensions

Definition 101. [finite separable field extensions] *for finite algebraic field extension,* E/k*, with* $[E : k]_s = [E : k]$*,* E*, said to be* separable over k

Definition 102. [separable algebraic elements] *for field,* k*,* α*, which is algebraic over* k *with* $k(\alpha)$ *being separable over* k*, said to be* separable over k

Proposition 30. [separability and multiple roots] *for field,* k*,* α*, which is algebraic over* k*, is separable over* k if and only if $\mathrm{Irr}(\alpha, k, X)$ *has no multiple roots*

Definition 103. [separable polynomials] *for field,* k*,* $f \in k[X]$ *with no multiple roots, said to be* separable

Lemma 12. *for tower of algebraic field extensions,* $k \subset F \subset K$*, if* $\alpha \in K$ *is separable over* k*, then* α *is separable over* F

Theorem 26. [finite separable field extensions] *for finite field extension,* E/k*,* E *is separable over* k if and only if *every element of* E *is separable over* k

Arbitrary separable field extensions

Definition 104. [arbitrary separable field extensions] *for (not necessarily finite) field extension, E/k, E, of which every finitely generated subextension is separable over k, $i.e.$,*

$$(\forall n \in \mathbf{N} \ \& \ \alpha_1, \ldots, \alpha_n \in E)\,(k(\alpha_1, \ldots, \alpha_n) \text{ is separable over } k)$$

said to be separable over k

Theorem 27. [separable field extensions] *for algebraic extension, E/k, E, which is generated by family of elements, $\{\alpha_\lambda\}_{\lambda\in\Lambda}$, with every α_λ is separable over k, is separable over k*

Theorem 28. [separable extensions are distinguished] *separable extensions form distinguished class of extensions*

Separable closure and conjugates

Definition 105. [separable closure] *for field, k, compositum of all separable extensions of k in given algebraic closure k^{a}, called* separable closure of k, *denoted by* k^{s} or k^{sep}

Definition 106. [conjugates of fields] *for algebraic field extension, E/k, and embedding of E, σ, in k^{a} over k, E^{σ}, called* conjugate of E in k^{a}

- smallest normal extension of k containing E is compositum of all conjugates of E in E^{a}

Definition 107. [conjugates of elements of fields] *for field, k, α being algebraic over k, and distinct embeddings, $\sigma_1, \ldots, \sigma_r$ of $k(\alpha)$ into k^{a} over k, $\alpha^{\sigma_1}, \ldots, \alpha^{\sigma_r}$, called* conjugates of α in k^{a}

- $\alpha^{\sigma_1}, \ldots, \alpha^{\sigma_r}$ are simply distinct roots of $\mathrm{Irr}(\alpha, k, X)$
- smallest normal extension of k containing one of these conjugates is simply $k(\alpha^{\sigma_1}, \ldots, \alpha^{\sigma_r})$

Prime element theorem

Theorem 29. [prime element theorem] *for finite algebraic field extension,* E/k*, exists* $\alpha \in E$ *such that* $E = k(\alpha)$ if and only if *exists only finite # fields,* F*, such that* $k \subset F \subset E$*; if* E *is separable over* k*, exists such element,* α

Definition 108. [primitive element of fields] *for finite algebraic field extension,* E/k*,* $\alpha \in E$ *with* $E = k(\alpha)$*, called* primitive element of E over k

Finite fields

Definition 109. [finite fields] *for every prime number, p, and integer, $n \geq 1$, exists finite field of order p^n, denoted by $\mathbf{F}_{p^n}$, uniquely determined as subfield of algebraic closure, $\mathbf{F}_p{}^{\mathrm{a}}$, which is splitting field of polynomial*

$$f_{p,n}(X) = X^{p^n} - X$$

and whose elements are roots of $f_{p,n}$

Theorem 30. [finite fields] *for every finite field, F, exist prime number, p, and integer, $n \geq 1$, such that $F = \mathbf{F}_{p^n}$*

Corollary 15. [finite field extensions] *for finite field, $\mathbf{F}_{p^n}$, and integer, $m \geq 1$, exists one and only one extension of degree, m, which is $\mathbf{F}_{p^{mn}}$*

Theorem 31. [multiplicative group of finite field] *multiplicative group of finite field is cyclic*

Automorphisms of finite fields

Definition 110. [Frobenius mapping] *mapping*

$$\varphi_{p,n} : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$$

defined by $x \mapsto x^p$, *called* Frobenius mapping

- $\varphi_{p,n}$ is (ring) homeomorphism with $\operatorname{Ker} \varphi_{p,n} = \{0\}$ since $\mathbf{F}_{p^n}$ is field, thus is injective (Proposition 17), and surjective because $\mathbf{F}_{p^n}$ is finite,
- thus, $\varphi_{p,n}$ is *isomorphism leaving* $\mathbf{F}_p$ *fixed*

Theorem 32. [group of automorphisms of finite fields] *group of automorphisms of* $\mathbf{F}_{p^n}$ *is cyclic of degree* n, *generated by* $\varphi_{p,n}$

Theorem 33. [group of automorphisms of finite fields over another finite field] *for prime number,* p, *and integers,* $m, n \geq 1$, *in any* $\mathbf{F}_p{}^{\mathrm{a}}$, $\mathbf{F}_{p^n}$ *is contained in* $\mathbf{F}_{p^m}$ if and only if n *divides* m, *i.e., exists* $d \in \mathbf{Z}$ *such that* $m = dn$, *in which case,* $\mathbf{F}_{p^m}$ *is* normal and separable *over* $\mathbf{F}_{p^n}$ *group of automorphisms of* $\mathbf{F}_{p^m}$ *over* $\mathbf{F}_{p^n}$ *is cyclic of order,* d, *generated by* $\varphi_{p,m}^n$

Galois Theory

What we will do to appreciate Galois theory

- study
  - group of automorphisms of finite (and infinite) Galois extension (at length)
  - give examples, $e.g.$, cyclotomic extensions, abelian extensions, (even) non-abelian ones
  - leading into study of matrix representation of Galois group & classifications

- have tools to prove
  - fundamental theorem of algebra
  - insolvability of quintic polynomials

- mention unsolved problems
  - given finite group, exists Galois extension of $\mathbf{Q}$ having this group as Galois group?

Fixed fields

Definition 111. [fixed fields] *for field, K, and group of automorphisms, G, of K,*

$$\{x \in K | \forall \sigma \in G, x^\sigma = x\} \subset K$$

is subfield of K, and called fixed field of G*, denoted by* K^G

- K^G is subfield of K because for every $x, y \in K^G$
  - $0^\sigma = 0 \Rightarrow 0 \in K^G$
  - $(x+y)^\sigma = x^\sigma + y^\sigma = x + y \Rightarrow x + y \in K^G$
  - $(-x)^\sigma = -x^\sigma = -x \Rightarrow -x \in K^G$
  - $1^\sigma = 1 \Rightarrow 1 \in K^G$
  - $(xy)^\sigma = x^\sigma y^\sigma = xy \Rightarrow xy \in K^G$
  - $(x^{-1})^\sigma = (x^\sigma)^{-1} = x^{-1} \Rightarrow x^{-1} \in K^G$

  hence, K^G closed under addition & multiplication, and is commutative division ring, thus field
- $0, 1 \in K^G$, hence K^G *contains prime field*

Galois extensions and Galois groups

Definition 112. [Galois extensions] *algebraic extension, K, of field, k, which is normal and separable, said to be* Galois (extension of k) *or* Galois over k *considering K as embedded in k^{a}; for convenience, sometimes say* K/k is Galois

Definition 113. [Galois groups] *for field, k and its Galois extension, K, group of automorphisms of K over k, called* Galois group of K over k, *denoted by* $G(K/k)$, $G_{K/k}$, $\mathrm{Gal}(K/k)$, or (simply) G

Definition 114. [Galois groups of polynomials] *for field, k, separable $f \in k[X]$ with $\deg f \geq 1$, and its splitting field, K/k, Galois group of K over k ($i.e.$, $G(K/k)$), called* Galois group of f over k

Proposition 31. [Galois groups of polynomials and symmetric groups] *for field, k, separable $f \in k[X]$ with $\deg f \geq 1$, and its splitting field, K/k,*

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$$

elements of Galois group of f over k, G, permute roots of f, hence, exists injective homeomorphism of G into S_n, $i.e.$, symmetric group on n elements

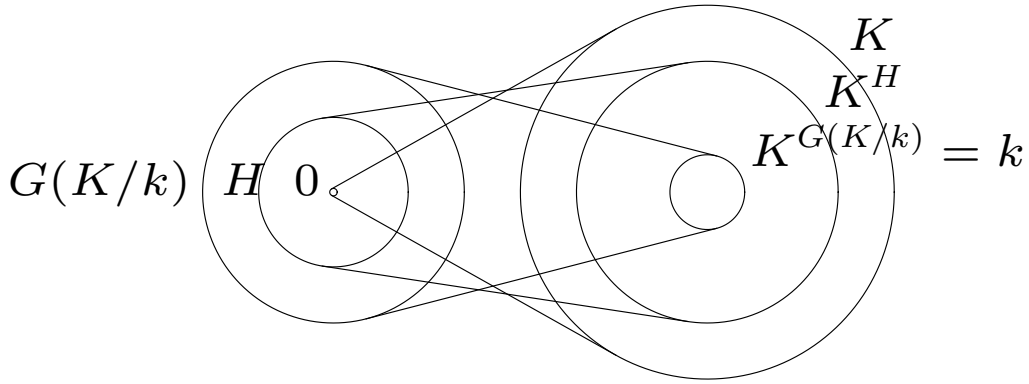
Fundamental theorem for Galois theory

Theorem 34. [fundamental theorem for Galois theory] *for finite Galois extension,* K/k

- *map* $H \mapsto K^H$ *induces isomorphism between set of subgroups of* $G(K/k)$ *& set of intermediate fields*
- *subgroup,* H*, of* $G(K/k)$*, is normal* if and only if K^H/k *is Galois*
- *for normal subgroup,* H*,* $\sigma \mapsto \sigma|K^H$ *induces isomorphism between* $G(K/k)/H$ *and* $G(K^H/k)$

(illustrated in figure)

- shall prove step by step



Galois subgroups association with intermediate fields

Theorem 35. [Galois subgroups associated with intermediate fields - 1] *for Galois extension, K/k, and intermediate field, F*

- *K/F is Galois & $K^{G(K/F)} = F$, hence, $K^G = k$*
- *map*

$$F \mapsto G(K/F)$$

induces injective *homeomorphism from set of intermediate fields to subgroups of G*

(proof can be found in Proof 8)

Definition 115. [Galois subgroups associated with intermediate fields] *for Galois extension, K/k, and intermediate field, F, subgroup, $G(K/F) \subset G(K/k)$, called* group associated with F*, said to* belong to F

Corollary 16. [Galois subgroups associated with intermediate fields - 1] *for Galois extension, K/k, and two intermediate fields, F_1 and F_2, $G(K/F_1) \cap G(K/F_2)$ belongs to F_1F_2, $i.e.$,*

$$G(K/F_1) \cap G(K/F_2) = G(K/F_1F_2)$$

(proof can be found in Proof 9)

Corollary 17. [Galois subgroups associated with intermediate fields - 2] *for Galois extension, K/k, and two intermediate fields, F_1 and F_2, smallest subgroup of G containing $G(K/F_1)$ and $G(K/F_2)$ belongs to $F_1 \cap F_2$, $i.e.$*

$$\bigcap_{G(K/F_1)\subset H, G(K/F_2)\subset H} \{H | H \subset G(K/k)\} = G(K/(F_1 \cap F_2))$$

Corollary 18. [Galois subgroups associated with intermediate fields - 3] *for Galois extension, K/k, and two intermediate fields, F_1 and F_2,*

$$F_1 \subset F_2 \text{ if and only if } G(K/F_2) \subset G(K/F_1)$$

(proof can be found in Proof 10)

Corollary 19. *for finite separable field extension, E/k, the smallest normal extension of k containing E, K, K/k is finite Galois and exist only finite number of intermediate fields*

Lemma 13. *for algebraic separable extension, E/k, if every element of E has degree no greater than n over k for some $n \geq 1$, E is finite over k and $[E : k] \leq n$*

Theorem 36. [Artin's theorem] *(Artin) for field, K, finite $\mathrm{Aut}(K)$ of order, n, and $k = K^{\mathrm{Aut}(K)}$, K/k is Galois, $G(K/k) = \mathrm{Aut}(K)$, and $[K : k] = n$*

Corollary 20. [Galois subgroups associated with intermediate fields - 4] *for finite Galois extension, K/k, every subgroup of $G(K/k)$ belongs to intermediate field*

Theorem 37. [Galois subgroups associated with intermediate fields - 2] *for Galois extension, K/k, and intermediate field, F,*

- *F/k is normal extension* if and only if *$G(K/F)$ is normal subgroup of $G(K/k)$*
- *if F/k is normal extension, map, $\sigma \mapsto \sigma|F$, induces homeomorphism of $G(K/k)$ onto $G(F/k)$ of which $G(K/F)$ is kernel, thus*

$$G(F/k) \approx G(K/k)/G(K/F)$$

Proof for fundamental theorem for Galois theory

- finally, we prove *fundamental theorem for Galois theory* (Theorem 34)
- assume K/k is finite Galois extension and H is subgroup of $G(K/k)$
  - Corollary 20 implies K^H is intermediate field, hence Theorem 35 implies K/K^H is Galois, Theorem 36 implies $G(K/K^H) = H$, thus, every H is Galois
  - map, $H \mapsto K^H$, induces homeomorphism, σ, of set of all subgroups of $G(K/k)$ into set of intermediate fields
  - σ is *injective* since for any two subgroups, H and H', of $G(K/k)$, if $K^H = K^{H'}$, then $H = G(K/K^H) = G(K/K^{H'}) = H'$
  - σ is *surjective* since for every intermediate field, F, Theorem 35 implies K/F is Galois, $G(K/F)$ is subgroup of $G(K/k)$, and $K^{G(K/F)} = F$, thus, $\sigma(G(K/F)) = K^{G(K/F)} = F$
  - *therefore, σ is isomorphism between set of all subgroups of $G(K/k)$ and set of intermediate fields*
  - since Theorem 28 implies separable extensions are distinguished, H^K/k is separable, thus Theorem 37 implies that K^H/k is Galois *if and only if* $G(K/K^H)$ is normal
  - lastly, Theorem 37 implies that if K^H/k is Galois, $G(H^K/k) \approx G(K/k)/H$

Abelian and cyclic Galois extensions and groups

Definition 116. [abelian Galois extensions] *Galois extension with abelian Galois group, said to be* abelian

Definition 117. [cyclic Galois extensions] *Galois extension with cyclic Galois group, said to be* cyclic

Corollary 21. *for Galois extension, K/k, and intermediate field, F,*

- *if K/k is abelian, F/k is Galois and abelian*
- *if K/k is cyclic, F/k is Galois and cyclic*

Definition 118. [maximum abelian extension] *for field, k, compositum of all abelian Galois extensions of k in given k^{a}, called* maximum abelian extension of k*, denoted by* k^{ab}

Theorems and corollaries about Galois extensions

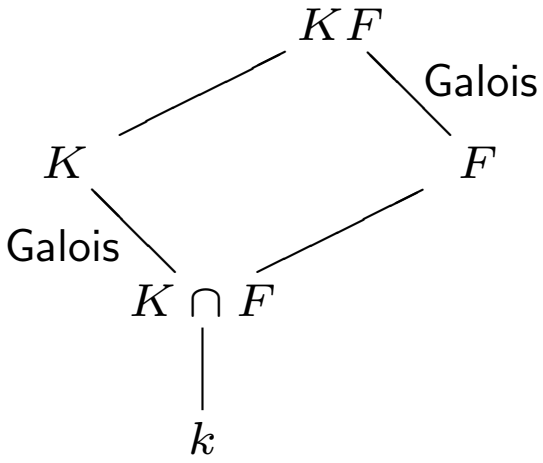
Theorem 38. *for Galois extension, K/k, and arbitrary extension, F/k, where K and F are subfields of common field,*

- *KF/F and $K/(K \cap F)$ are Galois extensions*
- *map*

$$\sigma \mapsto \sigma|K$$

induces isomorphism between $G(KF/F)$ and $G(K/(K \cap F))$

theorem illustrated in figure



Corollary 22. *for finite Galois extension, K/k, and arbitrary extension, F/k, where K and F are subfields of common field,*

$$[KF : F] \text{ divides } [F : k]$$

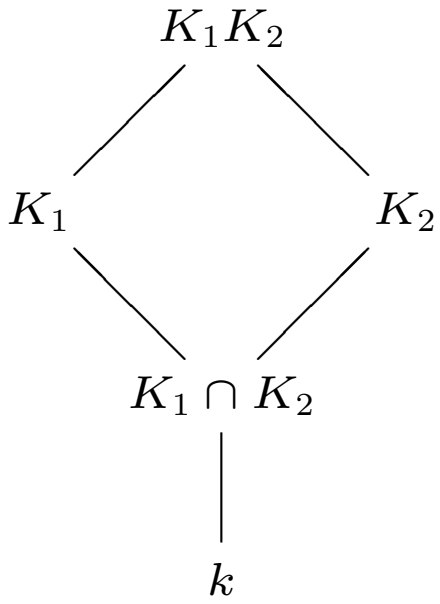
Theorem 39. *for Galois extensions, K_1/k and K_2/k, where K_1 and K_2 are subfields of common field,*

- *K_1K_2/k is Galois extension*
- *map*

  $$\sigma \mapsto (\sigma|K_1, \sigma|K_2)$$

  of $G(K_1K_2/k)$ into $G(K_1/k) \times G(K_2/k)$ is injective; if $K_1 \cap K_2 = k$, map is isomorphism

theorem illustrated in figure



Corollary 23. *for n Galois extensions, K_i/k, where $K_1, \ldots, K_n$ are subfields of common field and $K_{i+1} \cap (K_1 \cdots K_i) = k$ for $i = 1, \ldots, n-1$,*

- *$K_1 \cdots K_n/k$ is Galois extension*
- *map*

$$\sigma \mapsto (\sigma|K_1, \ldots, \sigma|K_n)$$

induces isomorphism of $G(K_1 \cdots K_n/k)$ onto $G(K_1/k) \times \cdots \times G(K_n/k)$

Corollary 24. *for Galois extension, K/k, where $G(K/k)$ can be written as $G_1 \times \cdots \times G_n$, and $K_1, \ldots, K_n$, each of which is fixed field of*

$$G_1 \times \cdots \times \underbrace{\{e\}}_{i\text{th position}} \times \cdots \times G_n$$

- $K_1/k, \ldots, K_n/k$ *are Galois extensions*
- $G(K_i/k) = G_i$ *for* $i = 1, \ldots, n$
- $K_{i+1} \cap (K_1 \cdots K_i) = k$ *for* $i = 1, \ldots, n-1$
- $K = K_1 \cdots K_n$

Theorem 40. *assume all fields are subfields of common field*

- *for two abelian Galois extensions, K/k and L/k, KL/k is abelian Galois extension*
- *for abelian Galois extension, K/k, and any extension, E/k, KE/E is abelian Galois extension*
- *for abelian Galois extension, K/k, and intermediate field, E, both K/E and E/k are abelian Galois extensions*

Solvable and radical extensions

Definition 119. [sovable extensions] *finite separable extension, E/k, such that Galois group of smallest Galois extension, K/k, containing E is solvable, said to be* solvable

Theorem 41. [solvable extensions are distinguished] *solvable extensions form distinguished class of extensions*

Definition 120. [solvable by radicals] *finite extension, F/k, such that it is separable and exists finite extension, E/k, containing F admitting tower decomposition*

$$k = E_0 \subset E_1 \subset \cdots \subset E_m = E$$

with E_{i+1}/E_i is obtained by adjoining root of

- *unity, or*
- *$X^n = a$ with $a \in E_i$, and n prime to characteristic, or*
- *$X_p - X - a$ with $a \in E_i$ if p is positive characteristic*

said to be solvable by radicals

Theorem 42. [extensions solvable by radicals] *separable extension, E/k, is solvable by radicals* if and only if *it is solvable*

Applications of Galois theory

Theorem 43. [insolvability of quintic polynomials] *general equation of degree, n, cannot be solved by radicals for $n \geq 5$ (implied by Definition 114, Proposition 31, Theorem 42, and Theorem 5)*

Theorem 44. [fundamental theorem of algebra] *$f \in \mathbf{C}[X]$ of degree, n, has precisely n roots in $\mathbf{C}$ (when counted with multiplicity), $i.e.$, $\mathbf{C}$ is algebraically closed*

Selected Proofs

Selected proofs

- **Proof 1.** *(Proof for "relation among coset indices" on page 20)*

  Let $\{h_1, \ldots, h_n\}$ and $\{k_1, \ldots, k_m\}$ be coset representations of H in G and K in H respectively. Then $n = (G : H)$ and $m = (H : K)$. Note that $\bigcup_{i,j} h_i k_j K = \bigcup_i h_i H = G$, and if $h_i k_j K = h_k k_l K$ for some $1 \leq i, k \leq n$ and $1 \leq j, k \leq m$, $h_i k_j K H = h_k k_l K H \Leftrightarrow h_i k_j H = h_k k_l H \Leftrightarrow h_i H = h_j H \Leftrightarrow h_i = h_j$, thus $k_j K = k_l K$, hence $k_j = k_l$. Thus $\{h_i k_j | 1 \leq i \leq n, 1 \leq j \leq m\}$ is cosets representations of K in G, therefore $(G : K) = mn = (G : H)(H : K)$. ∎

- **Proof 2.** *(Proof for "normality and commutativity of commutator subgroups" on page 34)*

  – For $a, x, y \in G$,

$$\begin{aligned} axyx^{-1}y^{-1} &= ax(a^{-1}x^{-1}xa)yx^{-1}y^{-1}(a^{-1}a) \\ &= (axa^{-1}x^{-1})(x(ay)x^{-1}(ay)^{-1})a \end{aligned}$$

and

$$\begin{aligned} xyx^{-1}y^{-1}a &= (aa^{-1})xyx^{-1}(ay^{-1}ya^{-1})y^{-1}a \\ &= \quad a((a^{-1}x)y(a^{-1}x)^{-1}y^{-1})(ya^{-1}y^{-1}a), \end{aligned}$$

hence commutator subgroup of G propagate every element of G from fron to back and vice versa. Therefore for every $a \in G$, $aG^C = G^C a$.

- For $x, y \in G$, $xG^C yG^C = xyG^C = G^C xy = (G^C x)(G^C y)$, hence G/G^C is commutative.
- For a homeomorphism of G, f, into a commutative group, and $x, y \in G$,

$$f(xyx^{-1}y^{-1}) = f(x)f(y)f(x^{-1})f(y^{-1}) = f(x)f(x^{-1})f(y)f(y^{-1}) = e$$

thus $xyx^{-1}y^{-1} \in \operatorname{Ker} f$, hence $G^C \subset \operatorname{Ker} f$.

∎

- **Proof 3.** *(Proof for "ideal generated by elements of ring" on page 57)*
For all $x \in (a_1, \ldots, a_n)$, and $y \in A$ $yx = y\left(\sum x_i a_i\right) = \sum (yx_i)a_i$ for some $\langle x_i \rangle_{i=1}^n \subset A$, hence $yx \in A$, and $(a_1, \ldots, a_n)$ is additive group, thus is ideal of A,

hence

$$\bigcap_{\mathfrak{a}:\text{ideal containing } a_1,\ldots,a_n} \mathfrak{a} \subset (a_1, \ldots, a_n)$$

Conversely, if $\mathfrak{a}$ contains $a_1, \ldots, a_n$, $Aa_i \subset \mathfrak{a}$, hence for every sequence, $\langle x_i \rangle_{i=1}^n \subset A$, $\sum x_i a_i \subset \mathfrak{a}$ because $\mathfrak{a}$ is additive subgroup of A, thus $(a_1, \ldots, a_n)$ is contained in every ideal containing $a_1, \ldots, a_n$, hence

$$(a_1, \ldots, a_n) \subset \bigcap_{\mathfrak{a}:\text{ideal containing } a_1,\ldots,a_n} \mathfrak{a}$$

∎

- **Proof 4.** *(Proof for "nonzero ideals of integers are principal" on page 67)*
  Suppose $\mathfrak{a}$ is a nonzero ideal of $\mathbf{Z}$. Because if negative integer, n, is in $\mathfrak{a}$, $-n$ is also in $\mathfrak{a}$ because $\mathfrak{a}$ is an additive group in the ring, $\mathbf{Z}$. Thus, $\mathfrak{a}$ has at least one positive integer. By Principle **??**, there exists the smallest positive integer in $\mathfrak{a}$. Let n be that integer. Let $m \in \mathfrak{a}$. By Theorem 13, there exist $q, r \in \mathbf{Z}$ such that $m = qn + r$ with $0 \leq r < n$. Since by the definition of ideals of rings, *i.e.*, Definition 45, $\mathfrak{a}$ is an additive group in $\mathbf{Z}$, hence $m - qn = r$ is also in $\mathfrak{a}$, thus r should be 0 because we assume n

is the smallest positive integer in $\mathfrak{a}$. Thus $\mathfrak{a} = \{qn | q \in \mathbf{Z}\} = n\mathbf{Z}$. Therefore the ideal is either $\{0\}$ or $n\mathbf{Z}$ for some $n > 0$. Both $\{0\}$ and $n\mathbf{Z}$ are ideal. ∎

- **Proof 5.** *(Proof for "algebraic-ness of smallest subfields" on page 100)*
  Proposition 25 implies that $k(\alpha_1) = k[\alpha_1]$ and $[k(\alpha_1) : k] = \deg \mathrm{Irr}(\alpha_1, k, X)$. Because α_2 is algebraic over k, hence algebraic over $k(\alpha_1)$ *a fortiori*, thus, the same proposition implies $k(\alpha_1, \alpha_2) = (k(\alpha_1))[\alpha_2] = (k[\alpha_1])[\alpha_2] = k[\alpha_1, \alpha_2]$ and $[k(\alpha_1, \alpha_2) : k(\alpha_1)] = \mathrm{Irr}(\alpha_2, k(\alpha_1), X)$, hence $[k(\alpha_1, \alpha_2) : k] = \mathrm{Irr}(\alpha_1, k, X)\,\mathrm{Irr}(\alpha_2, k(\alpha_1), X)$. The mathematical induction will surely prove that $k(\alpha_1, \ldots, \alpha_n) = k[\alpha_1, \ldots, \alpha_n]$ and

$$\begin{aligned}&[k(\alpha_1, \ldots, \alpha_n) : k] \\ &\quad = \quad \mathrm{Irr}(\alpha_1, k, X)\,\mathrm{Irr}(\alpha_2, k(\alpha_1), X) \cdots \mathrm{Irr}(\alpha_n, k(\alpha_1, \ldots, \alpha_{n-1}), X).\end{aligned}$$

  ∎

- **Proof 6.** *(Proof for "finite generation of compositum" on page 101)*
  First, it is obvious that $E = k(\alpha_1, \ldots, \alpha_n) \subset F(\alpha_1, \ldots, \alpha_n)$ and $F \subset F(\alpha_1, \ldots, \alpha_n)$, hence $EF \subset F(\alpha_1, \ldots, \alpha_n)$ because EF is defined to be the

smallest subfield that contains both E and F. Now every subfield containing both E and F contains all $f(\alpha_1, \ldots, \alpha_n)$ where $f \in F[X]$, hence all $f(\alpha_1, \ldots, \alpha_n)/g(\alpha_1, \ldots, \alpha_n)$ where $f, g \in F[X]$ and $g(\alpha_1, \ldots, \alpha_n) \neq 0$. Thus, $F(\alpha_1, \ldots, \alpha_n) \subset EF$ again by definition. Therefore $EF = F(\alpha_1, \ldots, \alpha_n)$. ∎

- **Proof 7.** *(Proof for "existence of algebraically closed algebraic extensions" on page 108)*

  Theorem 17 implies there exists an algebraically closed extension of k. Let E be such one. Let K be union of all algebraic extensions of k contained in E, then K is algebraic over k. Since k is algebraic over itself, K is not empty. Let $f \in K[X]$ with $\deg f \geq 1$. If α is a root of f, $\alpha \in E$. Since $K(\alpha)$ is algebraic over K and K is algebraic over k, $K(\alpha)$ is algebraic over k by Proposition 27. Therefore $K(\alpha) \subset K$ and $\alpha \in K$. Thus, K is algebraically closed algebraic extension of k. ∎

- **Proof 8.** *(Proof for "theorem - Galois subgroups associated with intermediate fields" on page 128)*

  Suppsoe $\alpha \in K^G$ and let $\sigma : k(\alpha) \to K^{\mathrm{a}}$ be an embedding inducing the identity on k. If we let $\tau : K \to K^{\mathrm{a}}$ extend σ, τ is automorphism by normality of K/k (Definition 99), hence $\tau \in G$, thus τ fixed α, which means σ is the identity, which is

the only embedding extension of the identity embedding of k onto itself to $k(\alpha)$, thus, by Definition 100,

$$[k(\alpha) : k]_s = 1.$$

Since K is separable over k, α is separable over k (by Theorem 26), and $k(\alpha)$ is separable over k (by Definition 102), thus $[k(\alpha) : k] = [k(\alpha) : k]_s = 1$, hence $k(\alpha) = k$, thus $\alpha \in k$, hence

$$K^G \subset k.$$

Since by definition, $k \subset K^G$, we have $K^G = k$.

Now since K/k is a normal extension, K/F is also a normal extension (by Theorem 23). Also, since K/k is a separable extension, K/F is also separable extension (by Theorem 28 and Definition 92). Thus, K/F is Galois (by Definition 112).

Now let F and F' be two intermediate fields. Since $K^{G(K/k)} = k$, we have $K^{G(K/F)} = F$ and $K^{G(K/F')} = F'$, thus if $G(K/F) = G(K/F')$, $F = F'$, hence the map is injective. ∎

- **Proof 9.** *(Proof for "Galois subgroups associated with intermediate fields - 1" on page 128)*

  First, K/F_1 and K/F_2 are Galois extensions by Theorem 35, hence $G(K/F_1)$ and

$G(K/F_2)$ can be defined. Also, Theorem 23 and Theorem 28 imply that K/F_1F_2 is Galois extension, hence $G(K/F_1F_2)$ can be defined, too.

Every automorphism of G leaving both F_1 and F_2 leaves F_1F_2 fixed, hence $G(K/F_1) \cap G(K/F_2) \subset G(K/F_1F_2)$. Conversely, every automorphism of G leaving F_1F_2 fxied leaves both F_1 and F_2 fixed, hence $G(K/F_1F_2) \subset G(K/F_1) \cap G(K/F_2)$.

Now we can do the same thing using rather mathematically rigorous terms. Assume that $\sigma \in G(K/F_1) \cap G(K/F_2)$. Then

$$(\forall x \in F_1, y \in F_2)\,(x^\sigma = x \;\&\; y^\sigma = y)\,,$$

thus

$$(\forall n, m \in \mathbf{N})$$
$$\left(\forall x_1, \ldots, x_n, x_1', \ldots, x_m' \in F_1, y_1, \ldots, y_n, y_1', \ldots, y_m' \in F_2\right)$$
$$\left(\left(\frac{x_1y_1 + \cdots + x_ny_n}{x_1'y_1' + \cdots + x_m'y_m'}\right)^\sigma = \frac{x_1y_1 + \cdots + x_ny_n}{x_1'y_1' + \cdots + x_m'y_m'}\right),$$

hence $\sigma \in G(K/F_1F_2)$, thus $G(K/F_1) \cap G(K/F_2) \subset\in G(K/F_1F_2)$. Conversely

if $\sigma \in G(K/F_1F_2)$,

$$(\forall x \in F_1, y \in F_2)\,(x^\sigma = x \;\&\; y^\sigma = y)\,,$$

hence $\sigma \in G(K/F_1) \cap G(K/F_2)$, thus $G(K/F_1) \cap G(K/F_2) \subset G(K/F_1F_2)$. ∎

- **Proof 10.** *(Proof for "Galois subgroups associated with intermediate fields - 3" on page 129)*

  First, K/F_1 and K/F_2 are Galois extensions by Theorem 35, hence $G(K/F_1)$ and $G(K/F_2)$ can be defined.

  If $F_1 \subset F_2$, every automorphism leaving F_2 fixed leaves F_1 fixed, hence it is in $G(K/F_1)$, thus $G(K/F_2) \subset G(K/F_1)$. Conversely, if $G(K/F_2) \subset G(K/F_1)$, every intermediate field $G(K/F_1)$ leaves fixed is left fixed by $G(K/F_2)$, hence $F_1 \subset F_2$.

  Now we can do the same thing using rather mathematically rigorous terms. Assume $F_1 \subset F_2$ and that $\sigma \subset G(K/F_2)$. Since Theorem 35 implies that

$$F_1 \subset F_2 = \{x \in K | (\forall \sigma \in G(K/F_2))(x^\sigma = x)\},$$

hence $(\forall x \in F_1)\,(x^\sigma = x)$, thus $\sigma \in G(K/F_1)$, hence

$$G(K/F_2) \subset G(K/F_1).$$

Conversely, assume that $G(K/F_2) \subset G(K/F_1)$. Then

$$\begin{aligned} F_1 &= \{x \in K | (\forall \sigma \in G(K/F_1))(x^\sigma = x)\} \\ &\subset \quad \{x \in K | (\forall \sigma \in G(K/F_2))(x^\sigma = x)\} = F_2 \end{aligned}$$

∎

Index

G
Galois groups
finite extensions, 126

G-set
groups, 43

$G(K/k)$
Galois groups
finite extensions, 126

$G_{K/k}$
Galois groups
finite extensions, 126

$\mathrm{Gal}(K/k)$
Galois groups
finite extensions, 126

p-Sylow subgroups of finite groups, 49

p-groups
groups, 49

p-subgroups
groups, 49

$\mathbf{Z}/n\mathbf{Z}$, 67

a fortiori algebraic-ness, 99

Abel, Niels Henrik
abelian groups, 14
abelian monoids, 13

abelian Galois extensions, 132

abelian groups, 14
towers, 31

abelian monoids, 13

abstract algebra, 10
history, 11
why, 10

action
groups, 43

addition
rings, 52

algebraic
extensions, 95
dimension, 96
over fields, 93
THE irreducible polynomial, 94

algebraic and finite extensions are distinguished, 104

algebraic closedness, 108
field, 108

algebraic closure, 110
fields, 110

algebraic embedding extensions, 109
fields, 109

algebraic extensions, 90, 95
field embeddings of, 106
Galois extensions, 126

algebraic over fields, 93

algebraic-ness of finite field extensions, 95

algebraic-ness of finitely generated subfields by multiple elements, 100

algebraic-ness of finitely generated subfields by single element, 99

algebraically closed, 85

fields, 85

almost everywhere - a.e., 6

alternating groups, 42
finite symmetric groups, 42

arbitrary separable field extensions, 118

Artin's theorem, 130

associativity
groups, 13

automorphism
groups, 16
monoids, 16

butterfly lemma
groups, 36

butterfly lemma - Zassenhaus, 36

canonical isomorphisms
groups, 27, 28

canonical maps
groups, 21
rings, 60

canonical maps of rings, 60

cardinality of algebraic extensions of infinite fields, 110

center
groups, 22
rings, 54

center of rings, 54

centralizers

groups, 22

characteristic
fields, 66
rings, 65

characteristic of rings, 65

Chinese remainder theorem, 69

class formula, 48
groups, 48

commutative groups, 14

commutative monoids, 13

commutative rings, 53

commutator, 34
groups, 34

commutator subgroups, 34
groups, 34

compositum
fields, 101
finite generation
fields, 101

compositum of subfields, 101

compositums
embedding, 106
fields, 106

compositums of fields, 106

congruence with respect to normal subgroup, 23
groups, 23

conjugate

groups, 44

conjugates of elements of fields, 119

conjugates of fields, 119

conjugation

groups, 44

conjugation of groups, 44

constant and monic polynomials, 80

constant polynomials, 80

convolution product

rings, 56

corollaries

existence of algebraically closed algebraic field extensions, 108

existence of extension fields containing roots, 108

finite dimensions of extensions, 96

finite field extensions, 121

Galois subgroups associated with intermediate fields - 1, 128

Galois subgroups associated with intermediate fields - 2, 129

Galois subgroups associated with intermediate fields - 3, 129

Galois subgroups associated with intermediate fields - 4, 130

induction of zero functions in multiple variables, 82

induction of zero functions in multiple variables - finite fields, 82

induction of zero functions in multiple variables - infinite fields, 82

induction of zero functions in one variable, 82

isomorphism between algebraically closed algebraic extensions, 109
isomorphism between splitting fields for family of polynomials, 112
isomorphism induced by Chinese remainder theorem, 69
multiplicative subgroup of finite field is cyclic, 84
uniqueness of reduced polynomials, 83

coset representation
groups, 19

cosets
groups, 19

cosets of groups, 19

countability of algebraic closure of finite fields, 110

cyclic Galois extensions, 132

cyclic generator
groups, 15

cyclic groups, 15
towers, 31

definitions
abelian Galois extensions, 132
algebraic closedness, 108
algebraic closure, 110
algebraic extensions, 95
algebraic over fields, 93
algebraically closed, 85
almost everywhere - a.e., 6
alternating groups, 42
arbitrary separable field extensions, 118
canonical maps of rings, 60
center of rings, 54

characteristic of rings, 65
commutative rings, 53
commutator, 34
commutator subgroups, 34
compositum of subfields, 101
congruence with respect to normal subgroup, 23

conjugates of elements of fields, 119
conjugates of fields, 119
conjugation of groups, 44
constant and monic polynomials, 80
cosets of groups, 19
cyclic Galois extensions, 132
cyclic groups, 15
derivatives of polynomials over commutative rings, 86
devision of entire ring elements, 72
dimension of extensions, 96
direct products, 15
distinguished class of field extensions, 103
division rings, 53
embedding of homeomorphism, 17
embedding of rings, 62
entire rings, 63
equivalent towers, 38
Euler phi-function, 68
evaluation homeomorphism, 76
exact sequences of homeomorphisms, 24
exponent of groups and group elements, 40
extensions of fields, 92
factor rings and residue classes, 60
factorial rings, 71
field embedding, 105
field embedding extensions, 105
fields, 53

finite fields, 121
finite separable field extensions, 117
finite tower of fields, 98
fixed fields, 125
Frobenius endomorphisms, 89
Frobenius mapping, 122
Galois extensions, 126
Galois groups, 126
Galois groups of polynomials, 126
Galois subgroups associated with intermediate fields, 128
generation of field extensions, 97
generators, 15
generators of ideals, 57
greatest common divisor (g.c.d.), 72
group rings, 56
groups, 14
groups of units of rings, 53
homeomorphism, 16
ideals, 57
index and order of groups, 19
induced injective ring-homeomorphisms, 62
infinitely often - i.o., 6
irreducible polynomials, 80
irreducible ring elements, 71
isotropy, 46
kernels of homeomorphism, 17
law of composition, 13
lifting, 102
maximal ideals, 64
maximum abelian extension, 132
monoids, 13
multiplicative groups of invertible elements of rings, 53

multiplicative subgroups of fields, 84
multiplicity and multiple roots, 87
normal extensions, 113
normal subgroups, 21
normalizers and centralizers, 22
operations of group on set, 43
orbits of operation, 47
period of group elements, 40
polynomial functions, 76
polynomials, 75
prime fields and prime rings, 66
prime ideals, 64
primitive n-th roots of unity, 84
primitive element of fields, 120
principal rings, 58
principals, 57
reduction maps, 78
reduction of f modulo p, 78
refinement of towers, 33
ring homeomorphisms, 59
rings, 52
rings of integers modulo n, 67
roots, 81
separable algebraic elements, 117
separable closure, 119
separable degree of field extensions, 115
separable polynomials, 117
simple groups, 35
solvable by radicals, 137
solvable groups, 33
sovable extensions, 137
splitting fields, 111
splitting fields for family of polynomials, 112
subrings, 53

sylow subgroups, 49
symmetric groups and permutations, 42
THE irreducible polynomial, 94
tower of fields, 98
towers of groups, 31
transitive operation, 47
translation, 45
unique factorization into irreducible elements, 71
variables and transcendentality, 76
zero divisors, 63

derivatives
of polynomials, 87
polynomials, 86

derivatives of polynomials, 87

derivatives of polynomials over commutative rings, 86

devision of entire ring elements, 72

dimension
algebraic extensions, 96
fields
algebraic extensions, 96

dimension of extensions, 96

dimension of finite extensions, 96

direct products, 15
groups, 15

distinguished class
fields
extensions, 103

distinguished class of field extensions, 103

division rings, 53

embedding
extensions
fields, 105
fields, 105
group homeomorphism, 17
rings, 62

embedding of homeomorphism, 17

embedding of rings, 62

embeddings of compositum of fields, 106

endomorphism
groups, 16
monoids, 16

entire rings, 63

equivalent towers, 38
groups, 38

Euclidean algorithm, 79
polynomials, 79

Euler
φ-function, 68
's theorem, 68
's totient function, 68
phi-function, 68

Euler φ-function, 68

Euler phi-function, 68

Euler's theorem, 68

Euler's totient function, 68

evaluation homeomorphism, 76

even
finite symmetric groups, 42

exact sequences of homeomorphisms, 24
groups, 24

existence of algebraically closed algebraic field extensions, 108

existence of algebraically closed field extensions, 108

existence of extension fields containing roots, 108

existence of greatest common divisor of principal entire rings, 72

existence of root of irreducible polynomials, 107

exponent
groups, 40

exponent of groups and group elements, 40

extensions
algebraic, 95
fields, 92
finite, 92
infinite, 92

extensions of fields, 92

extensions solvable by radicals, 137

factor groups
groups, 21

factor ring induced ring-homeomorphism, 61

factor rings
rings, 60

factor rings and residue classes, 60

factorial rings, 71

Feit
Feit-Thompson theorem, 33
Feit-Thompson theorem, 33
field embedding, 105
field embedding extensions, 105
field embeddings
of algebraic extensions, 106
field embeddings of algebraic extensions, 106
fields, 53
algebraic
over fields, 93
algebraic closedness, 108
algebraic closure, 110
algebraic embedding extensions, 109
algebraic extensions, 90, 91, 95
distinguished, 104
algebraic-ness
a fortiori, 99
finitely generated subfields by multiple elements, 100
finitely generated subfields by single element, 99
algebraically closed extensions, 85
cardinality of algebraic extensions of infinite fields, 110
characteristic, 66
compositum, 101
finite generation, 101
compositums, 106
countability of algebraic closure of finite fields, 110
dimension

extensions, 96
dimension of extensions
finiteness, 96
embedding, 105
compositums, 106
extensions, 105
existence of algebraically closed algebraic extensions, 108
existence of algebraically closed extensions, 108
existence of extension fields containing roots, 108
extensions, 92
algebraically closed algebraic, 108
distinguished class, 103
finite, 92, 95, 97
generation, 97
infinite, 92
extensions of fields, 92
finite extensions
distinguished, 104
finite tower of fields, 98
fixed fields, 125
generation of extensions, 97
having characteristic p, 88
isomorphic image of $\mathbf{Q}$ or $\mathbf{F}_p$, 66
isomorphism between algebraically closed algebraic extensions, 109
lifting, 102
multiplicative subgroups of fields, 84
number of algebraic embedding extensions, 109
prime, 66, 67
splitting, 111
isomorphism, 111
tower of fields, 98

finite dimensions of extensions, 96

finite extension is finitely generated, 97

finite field extensions, 121

finite fields, 121

finite generation of compositum, 101

finite groups, 14

finite multiplicative subgroups of field is cyclic, 84

finite separable field extensions, 117

finite solvable groups, 33

finite tower of fields, 98

fixed fields, 125

fixed points
    groups
        operation, 46

formula
    class formula, 48
    orbit decomposition formula, 48

Frobenius endomorphisms, 89
    polynomials, 89

Frobenius mapping, 122

fundamental theorem for Galois theory, 127

fundamental theorem of algebra, 138

g.c.d.
    rings, 72

Galois
    Galois extensions, 126
    Galois groups, 126

Galois theory, 127

Galois extensions, 126

algebraic extensions, 126

Galois groups, 126

Galois groups of polynomials, 126

Galois groups of polynomials and symmetric groups, 126

Galois subgroups associated with intermediate fields, 128

Galois subgroups associated with intermediate fields - 1, 128

Galois subgroups associated with intermediate fields - 2, 129, 130

Galois subgroups associated with intermediate fields - 3, 129

Galois subgroups associated with intermediate fields - 4, 130

Galois theory, 123, 124, 127

appreciation, 124

generated by

rings

ideals, 57

generation of field extensions, 97

generators, 15

groups, 15

generators of ideals, 57

rings, 57

greatest common divisor

principal entire rings, 72

rings, 72

greatest common divisor (g.c.d.), 72

rings, 72

group homeomorphism and isomorphism, 17

group of automorphisms of finite fields, 122

group of automorphisms of finite fields over another finite field, 122

group of invertible elements

rings, 53

group of units

rings, 53

group rings, 56

rings, 56

groups, 14

G-set, 43

p-groups, 49

p-subgroups, 49

abelian, 14

action, 43

associativity, 13

automorphism, 16

butterfly lemma, 36

canonical isomorphisms, 27, 28

canonical maps, 21

center, 22

centralizers, 22

class formula, 48

commutative, 14

commutator, 34

commutator subgroups, 34

congruence with respect to normal subgroup, 23

conjugate, 44
conjugation, 44
coset representation, 19
cosets, 19
cyclic, 15
cyclic generator, 15
cyclic groups, 15
direct products, 15
endomorphism, 16
equivalent towers, 38
exact sequences of homeomorphisms, 24
exponent, 40
factor groups, 21
finite, 14
Galois groups, 126
generators, 15
homeomorphism, 16
injective, 17
index, 19
inner, 44
isomorphism, 16
isotropy, 46
Jordan-Hölder theorem, 39
law of composition, 13
left cosets, 19
monoids, 13
normal subgroups, 21
normalizers, 22
operation, 43
faithful, 46
fixed points, 46
orbits, 47
transitive, 47
orbit decomposition formula, 48

order, 19
orthogonal subgroups, 18
period
elements, 40
permutations, 42
refinement of towers, 33
right cosets, 19
Schreier theorem, 39
simple, 35
solvable groups, 33
special linear groups, 22
sylow subgroups, 49
symmetric, 42
alternating, 42
even, 42
odd, 42
towers, 31
abelian, 31
cyclic, 31
equivalent, 38
normal, 31
translation, 45
unit element, 13

groups of units of rings, 53

Hölder
Jordan-Hölder theorem, 39

homeomorphism, 16
groups, 16
embedding, 17
injective, 17
kernels, 17
monoids, 16
rings, 59

kernel, 59

ideals, 57
rings
generators of, 57
left, 57
right, 57
two-sided, 57

index
dimensions of finite extensions, 96
groups, 19

index and order of groups, 19

indices and orders, 20

induced injective ring-homeomorphisms, 62

induction of zero functions in multiple variables, 82

induction of zero functions in multiple variables - finite fields, 82

induction of zero functions in multiple variables - infinite fields, 82

induction of zero functions in one variable, 82

infinitely often - i.o., 6

injective
homeomorphism
groups, 17

injectivity of field homeomorphisms, 59

inner
groups, 44

insolvability of quintic polynomials, 138

inverse

groups, 14

irreducible elements

rings

entire, 71

irreducible polynomials, 80

existence of roots, 107

irreducible ring elements, 71

isomorphism

groups, 16

monoids, 16

isomorphism between algebraically closed algebraic extensions, 109

fields, 109

isomorphism between splitting fields, 111

isomorphism between splitting fields for family of polynomials, 112

isomorphism induced by Chinese remainder theorem, 69

isomorphisms of endomorphisms of cyclic groups, 70

isotropy, 46

groups, 46

Jordan

Jordan-Hölder theorem, 39

Jordan-Hölder theorem, 39

kernel

rings

homeomorphism, 59

kernels
group homeomorphism, 17

kernels of homeomorphism, 17

law of composition, 13
groups, 13

left cosets
groups, 19

left ideals
rings, 57

lemmas
a fortiori algebraic-ness, 99
butterfly lemma - Zassenhaus, 36
compositums of fields, 106
embeddings of compositum of fields, 106
existence of root of irreducible polynomials, 107

field embeddings of algebraic extensions, 106
finite generation of compositum, 101
normality of subgroups of order p, 50
number of fixed points of group operations, 49
properties of prime and maximal ideals, 64

lifting, 102
fields, 102

maximal ideals, 64
properties, 64
rings, 64

maximum abelian extension, 132

modulo
rings of integers modulo n, 67

monic polynomials, 80

monoid-homeomorphism, 16

monoids, 13
- abelian, 13
- automorphism, 16
- commutative, 13
- endomorphism, 16
- groups, 13
- homeomorphism, 16
- isomorphism, 16

multiple roots
- polynomials, 87
  - necessary and sufficient conditions, 87

multiplication
- rings, 52

multiplicative group of finite field, 121

multiplicative groups of invertible elements of rings, 53

multiplicative subgroup of finite field is cyclic, 84

multiplicative subgroups of fields, 84

multiplicativity of separable degree of field extensions, 116

multiplicity
- polynomials, 87

multiplicity and multiple roots, 87

necessary and sufficient condition for multiple roots, 87

normal extensions, 113

normal groups

towers, 31

normal subgroups, 21
groups, 21

normal subgroups and factor groups, 21

normality of subgroups of order p, 50

normalizers
groups, 22

normalizers and centralizers, 22

normalizers of groups, 23

number of algebraic embedding extensions, 109
fields, 109

number of fixed points of group operations, 49

odd
finite symmetric groups, 42

operation
groups, 43
faithful, 46
fixed points, 46
orbits, 47
transitive, 47

operations of group on set, 43

orbit decomposition formula, 48
groups, 48

orbits
groups
operation, 47

orbits of operation, 47

order
groups, 19
orthogonal subgroups, 18
groups, 18
period
groups
elements, 40
period of elements of finite groups, 40
period of group elements, 40
permutations
groups, 42
transposition, 42
polynomial functions, 76
polynomials, 73, 75
algebraically closed, 85
constant, 80
derivatives, 86, 87
Euclidean algorithm, 79
evaluation homeomorphism, 76
Frobenius endomorphisms, 89
induction of zero functions
multiple variables, 82
one variable, 82
irreducible, 80
monic, 80
multiple roots, 87
necessary and sufficient conditions, 87
multiplicity, 87
over arbitrary commutative rings, 74
over field fields, 74
polynomial functions, 76

primitive n-th roots of unity, 84
principality of polynomial rings, 79
reduced polynomials, 83
reduction maps, 78
reduction of f modulo p, 78
rings, 74, 75
roots, 81
roots of polynomials, 81
substitution homeomorphism, 76
transcendental, 76
variables, 76
with integer coefficients, 74
zeros, 81

prime
fields, 66, 67
rings, 66

prime element theorem, 120

prime fields, 66

prime fields and prime rings, 66

prime ideals, 64
properties, 64
rings, 64

prime rings, 66

primitive n-th roots of unity, 84
polynomials, 84

primitive element of fields, 120

principal entire ring is factorial, 72

principal rings, 58

principality of polynomial rings, 79

principals, 57
rings, 57

properties of cyclic groups, 41

properties of prime and maximal ideals, 64

propositions
algebraic and finite extensions are distinguished, 104
algebraic-ness of finite field extensions, 95
algebraic-ness of finitely generated subfields by multiple elements, 100
algebraic-ness of finitely generated subfields by single element, 99
cosets of groups, 19
derivatives of polynomials, 87
dimension of finite extensions, 96
existence of extension fields containing roots, 108
existence of greatest common divisor of principal entire rings, 72
factor ring induced ring-homeomorphism, 61
finite extension is finitely generated, 97
finite solvable groups, 33
Galois groups of polynomials and symmetric groups, 126
group homeomorphism and isomorphism, 17
indices and orders, 20
injectivity of field homeomorphisms, 59
necessary and sufficient condition for multiple roots, 87
normal subgroups and factor groups, 21
normalizers of groups, 23
number of algebraic embedding extensions, 109
orthogonal subgroups, 18
period of elements of finite groups, 40
properties of cyclic groups, 41

separability and multiple roots, 117
sign homeomorphism of finite symmetric groups, 42
simple groups, 35
subgroups of cyclic groups, 40
towers inded by homeomorphism, 31

reduced polynomials, 83
uniqueness, 83

reduction map
rings, 78

reduction maps, 78
polynomials, 78
reduction of f modulo p, 78

reduction of f modulo p, 78

refinement of towers, 33
groups, 33

residue classes
rings, 60

retention of normality of extensions, 114

right cosets
groups, 19

right ideals
rings, 57

ring homeomorphisms, 59

rings, 52
addition, 52
canonical maps
rings, 60
characteristic, 65

Chinese remainder theorem, 69
isomorphism induced by, 69
commutative, 53
convolution product, 56
devision of elements, 72
division rings, 53
embedding, 62
entire, 63
devision of elements, 72
factorial, 71
irreducible elements, 71
unique factorization, 71
factor ring induced ring-homeomorphism, 61
factor rings, 60
factorial, 71
g.c.d, 72
generated by ideals, 57
generators of ideals, 57
greatest common divisor, 72
greatest common divisor (g.c.d.), 72
greatest common divisor of principal entire rings, 72
group of invertible elements, 53
group of units, 53
group rings, 56
homeomorphism, 59, 65
kernel, 59
ideals
left ideals, 57
maximal, 64
prime, 64
right ideals, 57
two-sided ideals, 57
induced injective ring-homeomorphisms, 62

integers, 67
isomorphism induced by Chinese remainder theorem, 69
isomorphisms of endomorphisms of cyclic groups, 70
maximal ideals, 64
properties, 64
multiplication, 52
of integers modulo n, 67
prime, 67
of polynomial differential operators, 74
polynomials, 74, 75
prime, 66
prime ideals, 64
properties, 64
principal, 58
principality of polynomial rings, 79
principals, 57
reduction map, 78
residue classes, 60
subrings, 53
units, 53
zero divisors, 63
rings of integers modulo n, 67
roots, 81
polynomials, 81
roots of polynomials, 81
Schreier, 39
Schreier theorem, 39
Schreier theorem
groups, 39
separability and multiple roots, 117

separable algebraic elements, 117

separable closure, 119

separable degree of field extensions, 115

separable extensions are distinguished, 118

separable field extensions, 118

separable polynomials, 117

sign homeomorphism of finite symmetric groups, 42

simple groups, 35

simplicity of alternating groups, 42

solvability condition in terms of normal subgroups, 33

solvability of finite p-groups, 50

solvability of finite symmetric groups, 42

solvable by radicals, 137

solvable extensions are distinguished, 137

solvable groups, 33
    groups, 33

sovable extensions, 137

special linear groups
    groups, 22

splitting fields, 111
    isomorphism, 111

splitting fields for family of polynomials, 112

subgroups, 14
    groups, 14

trivial, 14

subgroups of cyclic groups, 40

submonoids, 13

submonoidx
monoids, 13

subrings, 53
rings, 53

sylow subgroups, 49
groups, 49

symmetric groups
groups, 42
transposition, 42

symmetric groups and permutations, 42

THE irreducible polynomial, 94

theorems
p-Sylow subgroups of finite groups, 49
algebraic embedding extensions, 109
Artin's theorem, 130
cardinality of algebraic extensions of infinite fields, 110
Chinese remainder theorem, 69
countability of algebraic closure of finite fields, 110
Euclidean algorithm, 79
Euler's theorem, 68
existence of algebraically closed field extensions, 108
extensions solvable by radicals, 137
Feit-Thompson theorem, 33
finite fields, 121

finite multiplicative subgroups of field is cyclic, 84
finite separable field extensions, 117
fundamental theorem for Galois theory, 127
fundamental theorem of algebra, 138
Galois subgroups associated with intermediate fields - 1, 128
Galois subgroups associated with intermediate fields - 2, 130
group of automorphisms of finite fields, 122
group of automorphisms of finite fields over another finite field, 122
insolvability of quintic polynomials, 138
isomorphism between splitting fields, 111
isomorphisms of endomorphisms of cyclic groups, 70
multiplicative group of finite field, 121
multiplicativity of separable degree of field extensions, 116
normal extensions, 113
prime element theorem, 120
principal entire ring is factorial, 72
principality of polynomial rings, 79
retention of normality of extensions, 114
roots of polynomials, 81
Schreier, 39
separable extensions are distinguished, 118
separable field extensions, 118
simplicity of alternating groups, 42
solvability condition in terms of normal subgroups, 33
solvability of finite p-groups, 50
solvability of finite symmetric groups, 42
solvable extensions are distinguished, 137
upper limit on separable degree of field extensions, 116

Thompson
Feit-Thompson theorem, 33

tower of fields, 98

towers
abelian, 31
cyclic, 31
equivalent, 38
groups, 31
inded by homeomorphism, 31
normal, 31
refinement, 33

towers inded by homeomorphism, 31

towers of groups, 31

transitive
groups
operation, 47

transitive operation, 47

translation, 45
groups, 45

transpositions
permutations, 42
symmetric groups, 42

trivial subgroups, 14

two-sided ideals
rings, 57

unique factorization
rings
entire, 71

unique factorization into irreducible elements, 71

uniqueness of reduced polynomials, 83

unit
rings, 53

unit element
groups, 13

upper limit on separable degree of field extensions, 116

variables and transcendentality, 76

Zassenhaus
butterfly lemma, 36

zero divisors, 63
rings, 63

zeros
polynomials, 81

ZZ-figures
butterfly lemma, 37
commutative diagram, 29
commutative diagram for canonical homeomorphism, 30
commutative diagram for canonical isomorphism, 28
commutative diagram for canonical map, 25
diagram for Galois lifting, 133
diagram for Galois two-side lifting, 135
diagrams for Galois main result, 127
embedding extension, 105
factor-ring-induced-ring-homeomorphism, 61
lattice diagram of fields, 103
lifting or smallest fields, 102
translation or lifting of fields, 102

ZZ-important

for field, k, and its algebraic extension, E, embedding of E into itself over k is isomorphism , 106

algebraically closed algebraic extension is determined up to isomorphism, 109

group having an abelian tower whose last element is trivial subgroup, said to be *solvable*, 33

ZZ-todo

1 - convert proper bullet points to theorem, definition, lemma, corollary, proposition, etc., 0

5 - change comm conventions, 0

5 - change mathematicians' names, 0

CANCELLED - < 2024 0421 - python script extracting important list, 0

DONE - 2024 0324 - change tocpageref and funpageref to hyperlink, 0

DONE - 2024 0324 - python script extracting figure list -¿using list of figures functionality on doc, 0

DONE - 2024 0324 - python script extracting theorem-like list → using "list of theorem" functionality on doc, 0

DONE - 2024 0324 - python script for converting slides to doc, 0