

# Searching for Universal Truths

## Abstract Algebra

**Sunghee Yun**  
sunghee.yun@gmail.com

# Navigating Mathematical and Statistical Territories

- Notations & definitions & conventions
  - notations - 2
  - some definitions - 6
  - some conventions - 7
- Abstract algebra - 8
  - groups - 12
  - rings - 51
  - polynomials - 79
  - algebraic extension - 96
  - Galois theory - 130
- Proof & references & indices
  - selected proofs - 147
  - references - 166
  - index - 168

## Notations

- sets of numbers
  - $\mathbf{N}$  - set of natural numbers
  - $\mathbf{Z}$  - set of integers
  - $\mathbf{Z}_+$  - set of nonnegative integers
  - $\mathbf{Q}$  - set of rational numbers
  - $\mathbf{R}$  - set of real numbers
  - $\mathbf{R}_+$  - set of nonnegative real numbers
  - $\mathbf{R}_{++}$  - set of positive real numbers
  - $\mathbf{C}$  - set of complex numbers
- sequences  $\langle x_i \rangle$  and the like
  - finite  $\langle x_i \rangle_{i=1}^n$ , infinite  $\langle x_i \rangle_{i=1}^\infty$  - use  $\langle x_i \rangle$  whenever unambiguously understood
  - similarly for other operations, *e.g.*,  $\sum x_i$ ,  $\prod x_i$ ,  $\cup A_i$ ,  $\cap A_i$ ,  $\times A_i$
  - similarly for integrals, *e.g.*,  $\int f$  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  $A$
  - $A^\circ$  - interior of set  $A$
  - **relint**  $A$  - relative interior of set  $A$
  - **bd**  $A$  - boundary of set  $A$
- set algebra
  - $\sigma(\mathcal{A})$  -  $\sigma$ -algebra generated by  $\mathcal{A}$ , *i.e.*, smallest  $\sigma$ -algebra containing  $\mathcal{A}$
- norms in  $\mathbf{R}^n$ 
  - $\|x\|_p$  ( $p \geq 1$ ) -  $p$ -norm of  $x \in \mathbf{R}^n$ , *i.e.*,  $(|x_1|^p + \cdots + |x_n|^p)^{1/p}$
  - *e.g.*,  $\|x\|_2$  - 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
  - $\text{Tr}(A)$  - 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;  $A \succ 0 \Leftrightarrow A \in \mathbf{S}_{++}^n$
- sometimes, use Python script-like notations (with serious abuse of mathematical notations)
  - use  $f : \mathbf{R} \rightarrow \mathbf{R}$  as if it were  $f : \mathbf{R}^n \rightarrow \mathbf{R}^n$ , *e.g.*,

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

and

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

which corresponds to Python code `numpy.exp(x)` or `numpy.log(x)` where `x` is instance of `numpy.ndarray`, *i.e.*, numpy array

- use  $\sum x$  to mean  $\mathbf{1}^T x$  for  $x \in \mathbf{R}^n$ , *i.e.*

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

which corresponds to Python code `x.sum()` where `x` is numpy array

- use  $x/y$  for  $x, y \in \mathbf{R}^n$  to mean

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

which corresponds to Python code `x / y` where `x` and `y` are 1-d numpy arrays

- use  $X/Y$  for  $X, Y \in \mathbf{R}^{m \times n}$  to mean

$$\begin{bmatrix} X_{1,1}/Y_{1,1} & X_{1,2}/Y_{1,2} & \cdots & X_{1,n}/Y_{1,n} \\ X_{2,1}/Y_{2,1} & X_{2,2}/Y_{2,2} & \cdots & X_{2,n}/Y_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ X_{m,1}/Y_{m,1} & X_{m,2}/Y_{m,2} & \cdots & X_{m,n}/Y_{m,n} \end{bmatrix}$$

which corresponds to Python code `X / Y` where `X` and `Y` are 2-d numpy arrays

## 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  $(X, \mathcal{B}, \mu)$  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?**

## Why abstract algebra?

- it's fun!
- can understand *intrinsic structures* of algebraic objects
- allow us to solve *extremely practical problems* (depending on your definition of practicality)
  - e.g., can prove why root formulas for polynomials of order  $n \geq 5$  do not exist
- prepare us for pursuing further math topics such as
  - differential geometry
  - algebraic geometry
  - analysis
  - representation theory
  - algebraic number theory

## 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  $S \times S \rightarrow S$  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 any two unit elements  $e$  and  $f$ ,  $e = ef = f$ , 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 the unit element  $e$  and is itself monoid, called **submonoid**

## Groups

**Definition 5. [group]** *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*

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

*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  $f : M \rightarrow M'$  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**  $f : G \rightarrow G'$  is similarly monoid-homeomorphism
  - homeomorphism  $f : G \rightarrow G'$  where exists  $g : G' \rightarrow G$  such that  $f \circ g : G' \rightarrow G'$  and  $g \circ f : G \rightarrow G$  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 **Aut( $G$ )**

## Kernel, image, and embedding of homeomorphism

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

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

**Proposition 1. [group homeomorphism and isomorphism]**

- for group-homeomorphism  $f : G \rightarrow G'$ ,  $f(G) \subset G'$  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  $f : S \rightarrow G'$  has at most one extension to homeomorphism of  $G$  into  $G'$

## Orthogonal subgroups

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

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

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

*can generalize to finite number of subgroups,  $H_1, \dots, H_n$  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 group]** 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]** *for group  $G$  and two subgroups  $H$  and  $K \subset G$  with  $K \subset H$ ,*

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

*when  $K$  is trivial, we have*

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

*(proof can be found in [Proof 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*

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

*called normal subgroup of  $G$ , in which case*

- *set of cosets  $\{xH | x \in G\}$  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  $G \bmod H$*
- *$x \mapsto xH$  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  $G$ ,

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

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

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

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  $\mathbf{R} \setminus \{0\}$  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  $\text{Im } f = \text{Ker } g$*

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

*said to be exact*

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

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

*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  $\varphi$
- $0 \rightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \rightarrow 0$  is exact *if and only if*  $f$  injective,  $g$  surjective, and  $\text{Im } f = \text{Ker } g$

- if  $H = \text{Ker } g$  above,  $0 \rightarrow H \rightarrow G \rightarrow G/H \rightarrow 0$
- more precisely, exists commutative diagram as in the 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  $G$  &  $G'$  and homeomorphism  $f : G \rightarrow G'$  whose kernel is  $H$ , exists unique homeomorphism  $f_* : G/H \rightarrow G'$  with

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

where  $\varphi : G \rightarrow G/H$  is canonical map, and  $f_*$  is injective

- $f_*$  can be defined by  $xH \mapsto f(x)$
- $f_*$  *said to be induced by  $f$*
- $f_*$  induces isomorphism  $\lambda : G/H \rightarrow \text{Im } f$
- below sequence summarizes above statements

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

where  $j$  is inclusion

- for group  $G$ , subgroup  $H \subset G$ , and homeomorphism  $f : G \rightarrow G'$  whose kernel contains  $H$ , intersection of all normal subgroups containing  $H$ ,  $N$ , which is the smallest normal subgroup containing  $H$ , is contained in  $\text{Ker } f$ , i.e.,  $N \subset \text{Ker } f$ , and exists unique homeomorphism,  $f_* : G/N \rightarrow G'$  such that

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

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

- $f_*$  can be defined by  $xN \mapsto f(x)$
- $f_*$  *said to be 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*

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

this can be shown in the 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  $H \subset G$  and  $K \subset G$  with  $H$  contained in normalizer of  $K$ ,  $H \cap K$  is normal subgroup of  $H$ ,  $HK = KH$  is subgroup of  $G$ , exists surjective homeomorphism

$$H \rightarrow HK/K$$

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

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

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

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

as shown in the figure,

$$\begin{array}{ccc} G & \longrightarrow & G' \\ \uparrow & & \uparrow \\ f^{-1}(H') & \longrightarrow & H' \end{array}$$

$H$  is normal in  $G$  and kernel of homeomorphism

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

is  $H$  where  $\varphi$  is canonical map, hence we have injective homeomorphism

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

again called *canonical homeomorphism*, giving commutative diagram in the 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*

- *said to be normal if every  $G_{i+1}$  is normal in  $G_i$*
- *said to be abelian if normal and every factor group  $G_i/G_{i+1}$  is abelian*
- *said to be cyclic if normal and every factor group  $G_i/G_{i+1}$  is cyclic*

**Proposition 7. [towers inded by homeomorphism]** *for group homeomorphism  $f : G \rightarrow G'$  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*

$$G_i/G_{i+1} \rightarrow G'_i/G'_{i+1}$$

*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.

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

- $G^C$  is normal in  $G$
- $G/G^C$  is commutative
- $G^C$  is contained in kernel of every homomorphism of  $G$  into commutative group
  - (proof can be found in [Proof 2](#)) 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 a group and normal subgroups  $u$  and  $v$  of  $U$  and  $V$  respectively,*

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

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

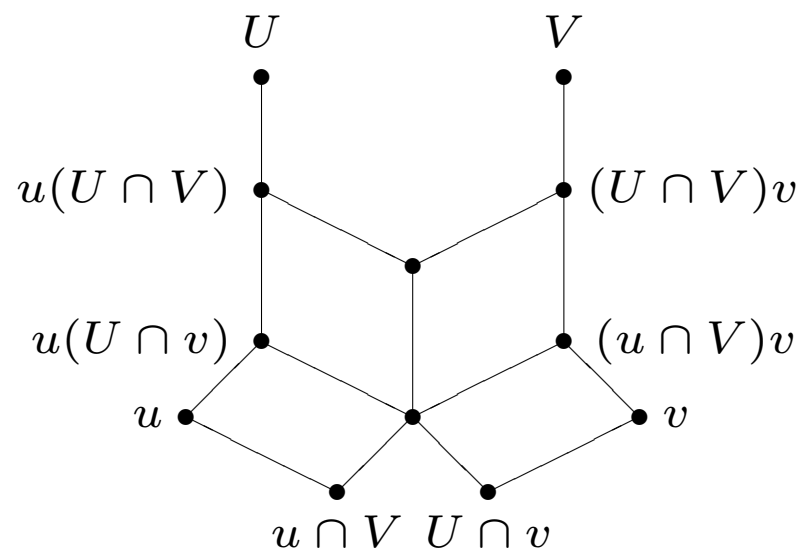
*and factor groups are isomorphic, i.e.,*

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

*these shown in the figure*

- indeed

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



## 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  $\pi \in \text{Perm}(\{1, \dots, n\})$ , 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 theorem]** *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 non-unit element  $a$  ( $\neq e$ ) divided  $n$ ; if  $n$  is prime number,  $G$  is cyclic and period of every generator is  $n$*

**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*

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

- *for cyclic group  $G$  and two generators  $a$  and  $b$ , 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  $\text{Perm}(S)$ ; elements in  $\text{Perm}(S)$  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  $S_n$ , exists unique homeomorphism  $\epsilon : S_n \rightarrow \{-1, 1\}$  mapping every transposition,  $\tau$ , to  $-1$ , i.e.,  $\epsilon(\tau) = -1$*

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

$$\pi : G \rightarrow \text{Perm}(S)$$

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

- $S$ , called  *$G$ -set*
- denote  $\pi(x)$  for  $x \in G$  by  $\pi_x$ , hence homeomorphism denoted by  $x \mapsto \pi_x$
- obtain mapping from such operation,  $G \times S \rightarrow S$ , with  $(x, s) \mapsto \pi_x(s)$
- often abbreviate  $\pi_x(s)$  by  $xs$ , with which the following two properties satisfied
  - $(\forall x, y \in G, s \in S) (x(y s) = (xy) s)$
  - $(\forall s \in S) (e s = s)$
- conversely, for mapping  $G \times S \rightarrow S$  with  $(x, s) \mapsto xs$  satisfying above two properties,  $s \mapsto xs$  is permutation for  $x \in G$ , hence  $\pi_x$  is homeomorphism of  $G$  into  $\text{Perm}(S)$
- thus, operation of  $G$  on  $S$  can be defined as mapping  $S \times G \rightarrow S$  satisfying above two properties

## Conjugation

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

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

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

- $\gamma_x$ , 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  $T_x : G \rightarrow G$  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,  $\text{Perm}(V)$
  - for  $V = F^n$ ,  $G$  is group of nonsingular  $n$ -by- $n$  matrices

## Isotropy

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

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

*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  $ys = s'$ ,

$$G_{s'} = yG_sy^{-1}$$

- 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  $G/G_s \rightarrow S$  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  $s_{\lambda}$  are elements of distinct orbits

**Formula 1. [orbit decomposition formula]** *for group  $G$  operating on set  $S$ , index set  $\Lambda$  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 exactly one fixed point,  $|S| \equiv 1 \pmod{p}$
- if  $p$  divides  $|S|$ ,  $|S| \equiv 0 \pmod{p}$

## 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  $G$  and smallest prime number dividing order of  $G$   $p$ , every subgroup of index  $p$  is normal*

**Proposition 16. [solvability of groups of order  $pq$ ]** *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. [ring]** 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  $xy + (-x)y = (x + -x)y = 0y = 0$

**Definition 37. [subring]** subset of ring which itself is ring with same additive and multiplicative laws of composition, called **subring**

## More on ring

**Definition 38. [multiplicative group of invertible elements of ring]** *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 39. [division ring]** *ring with  $1 \neq 0$  and every nonzero element being invertible, called **division ring***

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

**Definition 41. [center of ring]** *subset  $C \subset A$  of ring  $A$  such that*

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

*is subring, and is called **center of ring  $A$***

## Fields

**Definition 42. [field]** *commutative division ring, called field*

## General distributivity

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

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



## Ring examples

- for set  $S$  and ring  $A$ , *set of all mappings of  $S$  into  $A$*   $\text{Map}(S, A)$  whose addition and multiplication are defined as below, is *ring* (proof can be found in [Proof 3](#))

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

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

- additive and multiplicative unit elements of  $\text{Map}(S, A)$  are constant maps whose values are additive and multiplicative unit elements of  $A$  respectively
- $\text{Map}(S, A)$  is commutative *if and only if*  $A$  is commutative
- for set  $S$ ,  $\text{Map}(S, \mathbf{R})$  (page [2](#)) is a commutative ring
- for abelian group  $M$ , *set  $\text{End}(M)$  of group homeomorphisms of  $M$  into itself* is *ring* with normal addition and mapping composition as multiplication (proof can be found in [Proof 4](#))
  - additive and multiplicative unit elements of  $\text{End}(M)$  are constant map whose value is the unit element of  $M$  and identity mapping respectively

- not commutative in general
- for ring  $A$ , *set  $A[X]$  of polynomials over  $A$*  is *ring*, (Definition 70)
- for field  $K$ ,  $K^{n \times n}$ , *i.e.*, set of  $n$ -by- $n$  matrices with components in  $K$ , is *ring*
  - $(K^{n \times n})^*$ , *i.e.*, multiplicative group of units of  $K^{n \times n}$ , consists of non-singular matrices, *i.e.*, those whose determinants are nonzero

## Group ring

**Definition 43. [group ring]** 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  $K[G]$

- $\sum_{xy=z} a_x b_y$  above defines what is called **convolution product**

## Convolution product

**Definition 44. [convolution product]** *for two functions  $f, g$  on group  $G$ , convolution (product), denoted by  $f * g$ , defined by*

$$(f * g)(z) = \sum_{xy=z} f(x)f(y)$$

*as function on group  $G$*

- *one may restrict this definition to functions which are 0 except at finite number of elements*

- for  $f, g \in L^1(\mathbf{R})$ , can define convolution product  $f * g$  by

$$(f * g)(x) = \int_{\mathbf{R}} f(x - y)g(y)dy$$

– satisfies all axioms of ring except that there is not unit element

– commutative (essentially because  $\mathbf{R}$  is commutative)

- more generally, for locally compact group  $G$  with Haar measure  $\mu$ , can define *convolution product* by

$$(f * g)(x) = \int_G f(xy^{-1})g(y)d\mu(y)$$

## Ideals of ring

**Definition 45. [ideal]** 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, called **two-sided ideal** or simply **ideal**

- for ring  $A$ ,  $(0)$  and  $A$  itself are ideals

**Definition 46. [principal ideal]** for ring  $A$  and  $a \in A$ , left ideal  $Aa$ , called **principal left ideal**

- $a$ , said to be generator of  $\mathfrak{a} = Aa$  (over  $A$ )

**Definition 47. [principal two-sided ideal]**  $AaA$ , called **principal two-sided ideal** where

$$AaA = \bigcup_{i=1}^{\infty} \left\{ \sum_{i=1}^n x_i a y_i \mid x_i, y_i \in A \right\}$$

**Lemma 5. [ideals of field]** ideals of field only ideals of field are the field itself and zero ideal

## Principle rings

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

- $\mathbf{Z}$  (set of integers) is *principal* ring (proof can be found in [Proof 5](#))
- $k[X]$  (ring of polynomials) for field  $k$  is *principal* ring
- ring of algebraic integers in number field  $K$  is *not* necessarily principal
  - let  $\mathfrak{p}$  be prime ideal, let  $R_{\mathfrak{p}}$  be ring of all elements  $a/b$  with  $a, b \in R$  and  $b \notin \mathfrak{p}$ , then  $R_{\mathfrak{p}}$  is principal, with one prime ideal  $\mathfrak{m}_{\mathfrak{p}}$  consisting of all elements  $a/b$  as above but with  $a \in \mathfrak{p}$
- let  $A$  be set of entire functions on complex plane, then  $A$  is commutative ring, and every finitely generated ideal is *principal*
  - given discrete set of complex numbers  $\{z_i\}$  and nonnegative integers  $\{m_i\}$ , exists entire function  $f$  having zeros at  $z_i$  of multiplicity  $m_i$  and *no* other zeros
  - every principal ideal is of form  $Af$  for some such  $f$
  - group of units  $A^*$  in  $A$  consists of functions having no zeros

## Ideals as both additive and multiplicative monoids

- ideals form additive monoid
  - for left ideals  $\mathfrak{a}$ ,  $\mathfrak{b}$ ,  $\mathfrak{c}$  of ring  $A$ ,  $\mathfrak{a} + \mathfrak{b}$  is left ideal,  $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c})$ , hence form additive monoid with  $(0)$  as the unit element
  - similarly for right ideals & two-sided ideals
- ideals form multiplicative monoid
  - for left ideals  $\mathfrak{a}$ ,  $\mathfrak{b}$ ,  $\mathfrak{c}$  of ring  $A$ , define  $\mathfrak{a}\mathfrak{b}$  as

$$\mathfrak{a}\mathfrak{b} = \bigcup_{i=1}^{\infty} \left\{ \sum_{i=1}^n x_i y_i \mid x_i \in \mathfrak{a}, y_i \in \mathfrak{b} \right\}$$

then  $\mathfrak{a}\mathfrak{b}$  is also left ideal,  $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$ , hence form multiplicative monoid with  $A$  itself as the unit element; for this reason, this unit element  $A$ , *i.e.*, the ring itself, often written as  $(1)$

- similarly for right ideals & two-sided ideals
- ideal multiplication is also distributive over addition
- however, set of ideals does *not* form ring (because the additive monoid is *not* group)



## Generators of ideal

**Definition 49. [generators of ideal]** for ring  $A$  and  $a_1, \dots, a_n \in A$ , set of elements of  $A$  of form

$$\sum_{i=1}^n x_i a_i$$

with  $x_i \in A$ , is left ideal, denoted by  $(a_1, \dots, a_n)$ , 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  $a_i$

$$\bigcap_{a_1, \dots, a_n \in \mathfrak{a}} \mathfrak{a}$$

(proof can be found in [Proof 6](#)) - just like set  $(\sigma\text{-})$ algebras in set theory on page ??

## Entire rings

**Definition 50. [zero divisor]** *for ring  $A$ ,  $x, y \in A$  with  $x \neq 0$ ,  $y \neq 0$ , and  $xy = 0$ , said to be zero divisors*

**Definition 51. [entire ring]** *commutative ring with no zero divisors for which  $1 \neq 0$ , said to be entire; entire ring, sometimes called integral domain*

**Lemma 6. [every field is entire ring]** *every field is entire ring*

## Ring-homeomorphism

**Definition 52. [ring-homeomorphism]** *mapping of ring into ring  $f : A \rightarrow B$  such that  $f$  is monoid-homeomorphism for both additive and multiplicative structure on  $A$  and  $B$ , i.e.,*

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

*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  $f : A \rightarrow B$  is ideal of  $A$  (proof can be found in [Proof 7](#))*
- *conversely, for ideal  $\mathfrak{a}$ , can construct factor ring  $A/\mathfrak{a}$*
- *simply say “homeomorphism” if reference to ring is clear*

**Proposition 17. [injectivity of field homeomorphism]** *ring-homeomorphism from field into field is injective (due to [Lemma 5](#))*

## Factor ring and canonical map

**Definition 53. [factor ring and residue class]** for ring  $A$  and an ideal  $\mathfrak{a} \subset A$ , 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  $\mathfrak{a}$**

- for ring  $A$  and ideal  $\mathfrak{a}$ 
  - for subset  $S \subset \mathfrak{a}$ , write  $S \equiv 0 \pmod{\mathfrak{a}}$
  - for  $x, y \in A$ , if  $x - y \in \mathfrak{a}$ , write  $x \equiv y \pmod{\mathfrak{a}}$
  - if  $\mathfrak{a} = (a)$  for  $a \in A$ , for  $x, y \in A$ , if  $x - y \in \mathfrak{a}$ , write  $x \equiv y \pmod{a}$

**Definition 54. [canonical map of ring]** ring-homeomorphism of ring  $A$  into factor ring  $A/\mathfrak{a}$

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

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

## Factor ring induced ring-homeomorphism

**Proposition 18. [factor ring induced ring-homeomorphism]** *for ring-homeomorphism  $g : A \rightarrow A'$  whose kernel contains ideal  $\mathfrak{a}$ , exists unique ring-homeomorphism  $g_* : A/\mathfrak{a} \rightarrow A'$  making diagram in the figure commutative, i.e.,  $g_* \circ f = g$  where  $f$  is the ring canonical map  $f : A \rightarrow A/\mathfrak{a}$*

$$\begin{array}{ccc} A & \xrightarrow{g} & A' \\ & \searrow f & \nearrow g_* \\ & A/\mathfrak{a} & \end{array}$$

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

## Prime ideal and maximal ideal

**Definition 55. [prime ideal]** for commutative ring  $A$ , ideal  $\mathfrak{p} \neq A$  with  $A/\mathfrak{p}$  entire, called **prime ideal** or just **prime**;

- 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 56. [maximal ideal]** 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 7. [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
- 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

## Embedding of ring

**Definition 57. [ring-isomorphism]** *bijjective ring-homeomorphism (Definition 52) is isomorphism*

- indeed, for bijective ring-isomorphism  $f : A \rightarrow B$ , exists set-theoretic inverse  $g : B \rightarrow A$  of  $f$ , which is ring-homeomorphism

**Lemma 8. [image of ring-homeomorphism is subring]** *image  $f(A)$  of ring-homeomorphism  $f : A \rightarrow B$  is subring of  $B$  (proof can be found in Proof 8)*

**Definition 58. [embedding of ring]** *ring-isomorphism between  $A$  and its image, established by injective ring-homeomorphism  $f : A \rightarrow B$ , called embedding of ring*

**Definition 59. [induced injective ring-homeomorphism]** *for ring-homeomorphism  $f : A \rightarrow A'$  and ideal  $\mathfrak{a}'$  of  $A'$ , injective ring-homeomorphism*

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

*called induced injective ring-homeomorphism*

## Characteristic of ring

- for ring  $A$ , consider ring-homeomorphism

$$\lambda : \mathbf{Z} \rightarrow A$$

such that

$$\lambda(n) = ne$$

where  $e$  is multiplicative unit element of  $A$

- kernel of  $\lambda$  is ideal  $(n)$  for some  $n \geq 0$ , *i.e.*, ideal generated by some nonnegative integer  $n$
- hence, canonical injective ring-homeomorphism  $\mathbf{Z}/n\mathbf{Z} \rightarrow A$ , which is ring-isomorphism between  $\mathbf{Z}/n\mathbf{Z}$  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 60. [characteristic of ring]** *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 as subfield (isomorphic image of)
  - $\mathbf{Q}$  if characteristic is 0
  - $\mathbf{F}_p$  if characteristic is  $p$

**Definition 61. [prime field]** *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*

**Definition 62. [prime ring]** *in above cases, prime ring (contained in  $K$ ) means either integers  $\mathbf{Z}$  if  $K$  has characteristic 0 or  $\mathbf{F}_p$  if  $K$  has characteristic  $p$*

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

- $\mathbf{Z}$  is ring
- every ideal of  $\mathbf{Z}$  is principal, *i.e.*, either  $\{0\}$  or  $n\mathbf{Z}$  for some  $n \in \mathbf{N}$  (refer to page 62)
- ideal of  $\mathbf{Z}$  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 63.** [ring of integers modulo  $n$ ]  $\mathbf{Z}/n\mathbf{Z}$ , called ring of integers modulo  $n$ ; abbreviated as  $\text{mod } n$

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

## Euler phi-function

**Definition 64. [Euler phi-function]** for  $n > 1$ , order of division ring of  $\mathbf{Z}/n\mathbf{Z}$ , called 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  $p_i$  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  $n$  ideals  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  ( $n \geq 2$ ) with  $\mathfrak{a}_i + \mathfrak{a}_j = A$  for all  $i \neq j$*

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

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

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

*$f$  is surjective and  $\text{Ker } f = \bigcap \mathfrak{a}_i$ , hence, exists isomorphism*

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

## Isomorphism of endomorphisms of cyclic groups

**Theorem 11. [isomorphism 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*

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

- *group isomorphism*

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

where  $(\mathbf{Z}/n\mathbf{Z})^*$  denotes group of units of  $\mathbf{Z}/n\mathbf{Z}$  (Definition 38)

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

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

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

## Irreducibility and factorial rings

**Definition 65. [irreducible ring element]** *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 66. [unique factorization into irreducible elements]** *for entire ring  $A$ , element  $a \in A$  for which, exists unit  $u$  and irreducible elements,  $p_1, \dots, p_r$  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 67. [factorial ring]** *entire ring with every non-zero element has unique factorial into irreducible elements, called factorial ring or unique factorization ring*

## Greatest common divisor

**Definition 68. [division of entire ring elements]** *for entire ring  $A$  and nonzero elements  $a, b \in A$ ,  $a$  said to divide  $b$  if exists  $c \in A$  such that  $ac = b$ , denoted by  $a|b$*

**Definition 69. [greatest common divisor]** *for entire ring  $A$  and  $a, b \in A$ ,  $d \in A$  which divides  $a$  and  $b$  and satisfies*

$$(\forall c \in A) (c|a \ \& \ c|b \Rightarrow c|d)$$

*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 (ring 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
- *e.g.*, ring learning with errors (RLWE) for cryptographic algorithms

## Ring of polynomials

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

**Definition 70. [polynomial]** for ring  $A$ , set of functions from monoid  $S = \{X^r | r \in \mathbf{Z}, r \geq 0\}$  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  $aX^n$
- then, a polynomial can be uniquely written as

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

for some  $n \in \mathbf{Z}_+$ ,  $a_i \in A$

- $a_i$ , called **coefficients of  $f$**

## Polynomial functions

**Definition 71. [polynomial function]** 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  $f_B : B \rightarrow B$  defined by

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

called **polynomial function associated with  $f(X)$**

**Definition 72. [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,  $\text{ev}_b : f \mapsto f(b)$ , 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 73. [variables and transcendentality]** for two rings  $A$  and  $B$  with  $A \subset B$ , if  $x \in B$  makes evaluation homeomorphism  $\text{ev}_x : f \mapsto f(x)$  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  $\{a + b\alpha \mid a, b \in \mathbf{Z}\}$ , subring of  $\mathbf{Z}[\alpha] \subset \mathbf{R}$  generated by  $\alpha$ .
  - $\alpha$  is *not* transcendental because  $f(\alpha) = 0$  for  $f(X) = X^2 - 2$
  - hence kernel of evaluation map of  $\mathbf{Z}[X]$  into  $\mathbf{Z}[\alpha]$  is not injective, hence not isomorphism
  - indeed

$$\mathbf{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbf{Z}\}$$

- 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 nonzero  $x \in \mathbf{F}_p$  by Theorem 9 (Euler's theorem),  $x^p \equiv x$  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  $\varphi : A \rightarrow B$  of commutative rings, exists associated homeomorphisms of polynomial rings  $A[X] \rightarrow B[X]$  such that

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

**Definition 74. [reduction map]** *above ring homeomorphism  $f \mapsto \varphi f$ , called **reduction map***

- *e.g.*, for complex conjugate  $\varphi : \mathbf{C} \rightarrow \mathbf{C}$ , 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 75. [reduction of  $f$  modulo  $\mathfrak{p}$ ]** *for prime ideal  $\mathfrak{p}$  of ring  $A$  and surjective canonical map  $\varphi : A \rightarrow A/\mathfrak{p}$ , reduction map  $\varphi f$  for  $f \in A[X]$ , sometimes called **reduction of  $f$  modulo  $\mathfrak{p}$***

## 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 ring]** *polynomial ring in one variable  $k[X]$  with field  $k$  is principal*

**Corollary 3. [factoriality of polynomial ring]** *polynomial ring in one variable  $k[X]$  with field  $k$  is factorial*

## Constant, monic, and irreducible polynomials

**Definition 76. [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 77. [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**

## Roots or zeros of polynomials

**Definition 78. [root of polynomial]** *for commutative 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. [number of roots of polynomial]** *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 4. [induction of zero function in one variable]** *for field  $k$  and 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  $f = 0$ , i.e.,  $f$  induces zero function*

**Corollary 5. [induction of zero function 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*

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

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

**Corollary 6. [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 7. [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

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

for finite sequence,  $\langle a_i \rangle_{i=1}^m$ , and  $\langle \nu_{i,1} \rangle_{i=1}^m, \dots, \langle \nu_{i,n} \rangle_{i=1}^m$  where  $a_i \in k$  and  $\nu_{i,j} \geq 0$

- because  $X_i^q = X_i$  for any  $X_i$ , any  $\nu_{i,j} \geq q$  can be (repeatedly) replaced by  $\nu_{i,j} - (q - 1)$ , hence  $f$  can be rewritten as

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

where  $0 \leq \mu_{i,j} < q$  for all  $i, j$

**Definition 79. [reduced polynomials]** *above polynomial, called reduced polynomial, denoted by  $f^*$*

**Corollary 8. [uniqueness of reduced polynomials]** *for field  $k$  with  $q$  elements, reduced polynomial is unique (by Corollary 7)*

## Multiplicative subgroups and $n$ -th roots of unity

**Definition 80. [multiplicative subgroup of field]** *for field  $k$ , subgroup of group  $k^* = k \setminus \{0\}$ , called multiplicative subgroup of  $k$*

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

**Corollary 9. [multiplicative subgroup of finite field is cyclic]** *multiplicative subgroup of finite field is cyclic*

**Definition 81. [primitive  $n$ -th root 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  $\mu$ ; group of roots of unity in field  $k$ , denoted by  $\mu(k)$*

## Algebraic closedness

**Definition 82. [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 (Theorem 17)
- for algebraically closed field  $k$ 
  - (of course) 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 nonzero  $c \in k$ , distinct roots,  $\alpha_1, \dots, \alpha_r \in k$ , and  $m_1, \dots, m_r \in \mathbf{N}$

## Derivatives of polynomials

**Definition 83.** [derivative of polynomial over commutative ring] *for polynomial  $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$  with commutative ring  $A$ , map  $D : A[X] \rightarrow A[X]$  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  $a \in A$

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

## Multiple roots and multiplicity

- 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,  $g(a) \neq 0$ )

**Definition 84. [multiplicity and multiple roots]** *above,  $m$ , called **multiplicity of  $a$  in  $f$** ;  $a$ , said to be **multiple root of  $f$**  if  $m > 1$*

**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  $f(a) = 0$  and  $f'(a) = 0$*

**Proposition 21. [derivative of polynomial]** *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  $\nu$  whenever  $a_{\nu} \neq 0$*

## Frobenius endomorphism

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

## Roots with multiplicity $p^r$ in fields having characteristic $p$

- for field  $K$  having characteristic  $p$

- $p \mid \binom{p}{\nu}$  for all  $0 < \nu < p$  because  $p$  is prime, hence, for every  $a, b \in K$

$$(a + b)^p = a^p + b^p$$

- applying this resurvely  $r$  times yields

$$(a + b)^{p^r} = (a^p + b^p)^{p^{r-1}} = (a^{p^2} + b^{p^2})^{p^{r-2}} = \cdots = a^{p^r} + b^{p^r}$$

hence

$$(X - a)^{p^r} = X^{p^r} - a^{p^r}$$

- if  $a, c \in K$  satisfy  $a^{p^r} = c$

$$X^{p^r} - c = X^{p^r} - a^{p^r} = (X - a)^{p^r}$$

hence, polynomial  $X^{p^r} - c$  has precisely one root  $a$  of multiplicity  $p^r$ !



# **Algebraic Extension**

## Algebraic extension

- will show
  - for polynomial over field, always exists some extension of *that* field where the polynomial has root
  - existence of algebraic closure for every field

## Extension of field

**Definition 86. [extension of field]** for field  $E$  and its subfield  $F \subset E$ ,  $E$  said to be **extension field of  $F$** , (sometimes) denoted by  $E/F$  (which should not confused with factor group)

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

## Algebraic over field

**Definition 87. [algebraic over field]** *for field  $E$  and its subfield  $F \subset E$ ,  $\alpha \in E$  satisfying*

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

*said to be algebraic over  $F$*

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

• equivalent statements to Definition 87

– exists homeomorphism  $\varphi : F[X] \rightarrow E$  such that

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

– exists evaluation homeomorphism  $\text{ev}_\alpha : F[X] \rightarrow E$  with nonzero kernel (refer to Definition 72 for definition of evaluation homeomorphism)

- in which case,  $\text{Ker } \varphi$  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 (Lemma 6), hence  $p(X)$  irreducible (refer to Definition 55)

**Definition 88. [THE irreducible polynomial]** *normalized  $p(X)$  (i.e., with leading coefficient being 1) uniquely determined by  $\alpha$ , called THE irreducible polynomial of  $\alpha$  over  $F$ , denoted by  $\text{Irr}(\alpha, F, X)$*

## Algebraic extensions

**Definition 89. [algebraic extension]** *for field  $F$ , its extension field every element of which is algebraic over  $F$ , said to be algebraic extension of  $F$*

**Proposition 22. [algebraicness of finite field extensions]** *for field  $F$ , every finite extension field of  $F$  is algebraic over  $F$*

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

## Dimension of extensions

**Definition 90. [dimension of extension]** for field  $F$  and its extension field  $E$ , dimension of  $E$  as vector space over  $F$ , called **dimension of  $E$  over  $F$** , denoted by  $[E : F]$

**Proposition 23. [dimension of finite extension]** 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 10. [finite dimension of extension]** for field  $k$  and its extension fields  $F$  &  $E$  with  $k \subset F \subset E$ ,  $E/k$  is finite if and only if both  $F/k$  and  $E/F$  are finite

## Generation of field extensions

**Definition 91. [generation of field extensions]** for field  $k$ , its extension field  $E$ , and  $\alpha_1, \dots, \alpha_n \in E$ , smallest subfield containing  $k$  and  $\alpha_1, \dots, \alpha_n$ , said to be **finitely generated over  $k$  by  $\alpha_1, \dots, \alpha_n$** , denoted by  $k(\alpha_1, \dots, \alpha_n)$

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

$$\begin{aligned} k(\alpha_1, \dots, \alpha_n) \\ = \{ f(\alpha_1, \dots, \alpha_n)/g(\alpha_1, \dots, \alpha_n) \mid f, g \in k[X], g(\alpha_1, \dots, \alpha_n) \neq 0 \} \end{aligned}$$

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

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

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



## Tower of fields

**Definition 92. [tower of fields]** *sequence of extension fields*

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

*called tower of fields*

**Definition 93. [finite tower of fields]** *tower of fields, said to be finite if and only if each step of extensions is finite*

## Algebraicness of finitely generated subfields

**Proposition 25.** [algebraicness of finitely generated subfield by single element] *for field  $k$ , its extension field  $E$ , and  $\alpha \in E$  being algebraic over  $k$*

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

*and*

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

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

**Lemma 9.** [a fortiori algebraicness] *for field  $k$ , its extension field  $F$ , and  $\alpha \in E$  being algebraic over  $k$  where  $k(\alpha)$  and  $F$  are subfields of common field,  $\alpha$  is algebraic over  $F$*

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

- assume tower of fields

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

where  $\alpha_i$  is algebraic over  $k$

- then,  $\alpha_{i+1}$  is algebraic over  $k(\alpha_1, \dots, \alpha_i)$  (by Lemma 9)

**Proposition 26. [algebraicness of finitely generated subfields by multiple elements]**  
 for field  $k$  and  $\alpha_1, \dots, \alpha_n$  being algebraic over  $k$ ,  $E = k(\alpha_1, \dots, \alpha_n)$  is finitely algebraic over  $k$  (due to Proposition 25, Proposition 23, and Proposition 22). Indeed,  $E = k[\alpha_1, \dots, \alpha_n]$  and

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

(proof can be found in Proof 9)

## Compositum of subfields and lifting

**Definition 94. [compositum of subfields]** *for field  $k$  and its extension fields  $E$  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  $L$*

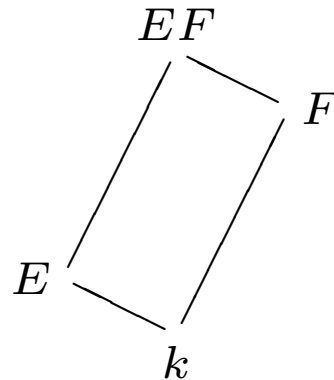
- could define **compositum of set of subfields of  $L$**  as smallest subfield containing subfields in the set

**Lemma 10.** *extension  $E$  of  $k$  is compositum of all its finitely generated subfields over  $k$ , i.e.,  $E = \bigcup_{n \in \mathbf{N}} \bigcup_{\alpha_1, \dots, \alpha_n \in E} k(\alpha_1, \dots, \alpha_n)$*

## Lifting

**Definition 95. [lifting]** *extension  $EF$  of  $F$ , called translation of  $E$  to  $F$  or lifting of  $E$  to  $F$*

- *often draw diagram as in the figure*



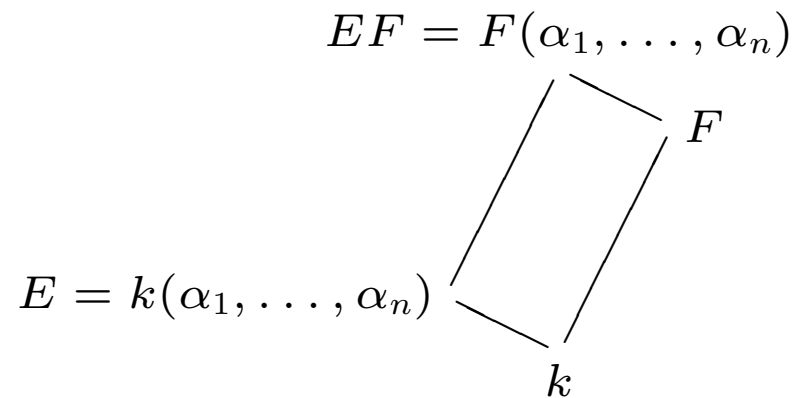
## Finite generation of compositum

**Lemma 11. [finite generation of compositum]** *for field  $k$ , its extension field  $F$ , and  $E = k(\alpha_1, \dots, \alpha_n)$  where both  $E$  and  $F$  are contained in common field  $L$ ,*

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

*i.e., compositum  $EF$  is finitely generated over  $F$  (proof can be found in [Proof 10](#))*

*- refer to diagra in the figure*



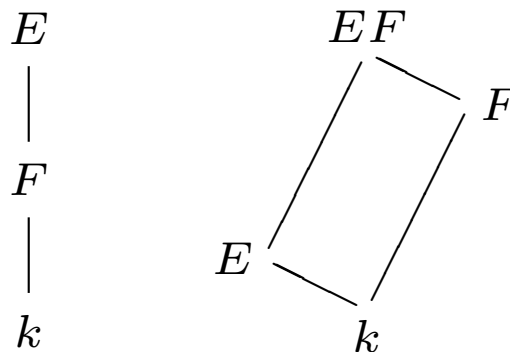
## Distinguished classes

**Definition 96. [distinguished class of field extensions]** *for field  $k$ , 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  $\mathcal{C}$*

*said to be distinguished; the figure illustrates these two properties, which imply the following property*

- *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  $\mathcal{C}$*



## 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*

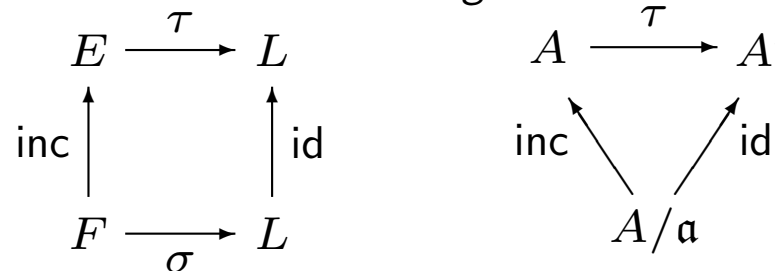
- true that finitely generated extensions form distinguished class (not necessarily algebraic extensions or finite extensions)



## Field embedding and embedding extension

**Definition 97. [field embedding]** for two fields  $F$  and  $L$ , injective homeomorphism  $\sigma : F \rightarrow L$ , called **embedding of  $F$  into  $L$** ; then (of course)  $\sigma$  induces isomorphism of  $F$  with its image  $\sigma F$ <sup>1</sup>

**Definition 98. [field embedding extension]** for field embedding  $\sigma : F \rightarrow L$ , field extension  $F \subset E$ , and embedding  $\tau : E \rightarrow L$  whose restriction to  $F$  being equal to  $\sigma$ , said to **be over  $\sigma$**  or **extend  $\sigma$** ; if  $\sigma$  is identity, embedding  $\tau$ , called **embedding of  $E$  over  $F$** ; diagrams in the figure show these embedding extensions



- assuming  $F$ ,  $E$ ,  $\sigma$ , and  $\tau$  same as in Definition 98, if  $\alpha \in E$  is root of  $f \in F[X]$ , then  $\alpha^\tau$  is root of  $f^\sigma$  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  $0 = f(\alpha)^\tau = \sum_{i=0}^n (a_i^\tau) (\alpha^\tau)^i = \sum_{i=0}^n a_i^\sigma (\alpha^\tau)^i = f^\sigma(\alpha^\tau)$

---

<sup>1</sup>Here  $\sigma F$  is sometimes written as  $F^\sigma$ .

## Embedding of field extensions

**Lemma 12. [field embedding of algebraic extension]** *for field  $k$  and its algebraic extension  $E$ , embedding of  $E$  into itself over  $k$  is isomorphism*

**Lemma 13. [compositums of fields]** *for field  $k$  and its field extensions  $E$  and  $F$  contained in common field,*

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

*and  $EF$  is field of quotients of these elements*

**Lemma 14. [embeddings of compositum of fields]** *for field  $k$ , its field extensions  $E_1$  and  $E_2$  contained in common field  $E$ , and embedding  $\sigma : E \rightarrow L$  for field  $L$ ,*

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

## Existence of roots of irreducible polynomial

- assume  $p(X) \in k[X]$  irreducible polynomial and consider canonical map, which is ring homeomorphism

$$\sigma : k[X] \rightarrow k[X]/((p(X)))$$

- consider  $\text{Ker } \sigma|_k$ 
  - every kernel of ring homeomorphism is ideal, hence if nonzero  $a \in \text{Ker } \sigma|_k$ ,  $1 \in \text{Ker } \sigma|_k$  because  $a^{-1} \in \text{Ker } \sigma|_k$ , but  $1 \notin ((p(X)))$
  - thus,  $\text{Ker } \sigma|_k = \{0\}$ , hence  $p^\sigma \neq 0$

- now for  $\alpha = X^\sigma$

$$p^\sigma(\alpha) = p^\sigma(X^\sigma) = (p(X))^\sigma = 0$$

- thus,  $\alpha$  is algebraic in  $k^\sigma$ , i.e.,  $\alpha \in k[X]^\sigma$  is root of  $p^\sigma$  in  $k^\sigma(\alpha)$

**Lemma 15. [existence of roots of irreducible polynomial]** *for field  $k$  and irreducible  $p(X) \in k[X]$  with  $\deg p \geq 1$ , exist field  $L$  and homeomorphism  $\sigma : k \rightarrow L$  such that  $p^\sigma$  with  $\deg p^\sigma \geq 1$  has root in field extension of  $k^\sigma$*

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

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

**Corollary 12.** [existence of algebraically closed algebraic field extensions] *for every field  $k$ , exists algebraically closed algebraic extension of  $k$  (proof can be found in [Proof 11](#))*

## Isomorphism between algebraically closed algebraic extensions

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

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

**Corollary 13. [isomorphism between algebraically closed algebraic extensions]** *for field,  $k$ , and its algebraically closed algebraic extensions,  $E$  and  $E'$ , exists isomorphism between  $E$  and  $E'$  which induces identity on  $k$ , i.e.*

$$\tau : E \rightarrow E'$$

where  $\tau|_k$  is identity

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

## Algebraic closure

**Definition 99. [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.*,  $\mathbf{Q}^a$
  - $\mathbf{Q}^a \neq \mathbf{C}$
  - $\mathbf{R}^a = \mathbf{C}$
  - $\mathbf{Q}^a$  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 100. [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  $\alpha_1, \dots, \alpha_n$  (hence  $K = k(\alpha_1, \dots, \alpha_n)$ ), 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  $k \subset K \subset k^a$ , every embedding of  $E$  into  $k^a$  over  $k$  is isomorphism of  $E$  onto  $K$

## Splitting fields for family of polynomials

**Definition 101. [splitting fields for family of polynomials]** *for field,  $k$ , index set,  $\Lambda$ , and indexed family of polynomials,  $\{f_\lambda \in k[X] \mid \lambda \in \Lambda, \deg f_\lambda \geq 1\}$ , extension field of  $k$ , every  $f_\lambda$  splits into linear factors in which and which is generated by all roots of all polynomials,  $f_\lambda$ , called **splitting field for family of polynomials***

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

**Corollary 14. [isomorphism between splitting fields for family of polynomials]** *for field,  $k$ , index set,  $\Lambda$ , and two splitting fields,  $K$  and  $E$ , for family of polynomials,  $\{f_\lambda \in k[X] \mid \lambda \in \Lambda, \deg f_\lambda \geq 1\}$ , 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  $k \subset K \subset k^a$ , 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 102. [normal extensions]** *for field,  $k$ , and its algebraic extension,  $K$ , with  $k \subset K \subset k^a$ , 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,  $\sigma : F \rightarrow L$ 
    - exists embedding extension of  $\sigma$  to  $E$  in  $L$  by Theorem 18
    - such  $\sigma$  maps  $E$  on subfield of  $L$  which is algebraic over  $F^\sigma$
    - hence,  $E^\sigma$  is contained in algebraic closure of  $F^\sigma$  which is contained in  $L$
    - will *assume* that  $L$  is the algebraic closure of  $F^\sigma$
  - let  $L'$  be another algebraically closed field and assume another embedding,  $\tau : F \rightarrow L'$  - assume as before that  $L'$  is algebraic closure of  $F^\tau$
  - then Theorem 18 implies, exists isomorphism,  $\lambda : L \rightarrow L'$  extending  $\tau \circ \sigma^{-1}$  applied to  $F^\sigma$
  - let  $S_\sigma$  &  $S_\tau$  be sets of embedding extensions of  $\sigma$  to  $E$  in  $L$  and  $L'$  respectively
  - then  $\lambda$  induces map from  $S_\sigma$  into  $S_\tau$  with  $\tilde{\sigma} \mapsto \lambda \circ \tilde{\sigma}$  and  $\lambda^{-1}$  induces inverse map from  $S_\tau$  into  $S_\sigma$ , hence exists bijection between  $S_\sigma$  and  $S_\tau$ , hence have same cardinality

**Definition 103. [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 15.** *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 104. [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 105. [separable algebraic elements]** *for field,  $k$ ,  $\alpha$ , 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,  $k$ ,  $\alpha$ , which is algebraic over  $k$ , is separable over  $k$  if and only if  $\text{Irr}(\alpha, k, X)$  has no multiple roots*

**Definition 106. [separable polynomials]** *for field,  $k$ ,  $f \in k[X]$  with no multiple roots, said to be separable*

**Lemma 16.** *for tower of algebraic field extensions,  $k \subset F \subset K$ , if  $\alpha \in K$  is separable over  $k$ , then  $\alpha$  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 107. [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.,*

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

*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  $\alpha_\lambda$  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 108. [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  $k^{\text{sep}}$

**Definition 109. [conjugates of fields]** for algebraic field extension,  $E/k$ , and embedding of  $E$ ,  $\sigma$ , in  $k^a$  over  $k$ ,  $E^\sigma$ , 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 110. [conjugates of elements of fields]** for field,  $k$ ,  $\alpha$  being algebraic over  $k$ , and distinct embeddings,  $\sigma_1, \dots, \sigma_r$  of  $k(\alpha)$  into  $k^a$  over  $k$ ,  $\alpha^{\sigma_1}, \dots, \alpha^{\sigma_r}$ , called **conjugates of  $\alpha$  in  $k^a$**

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

## 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,  $\alpha$*

**Definition 111. [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 112. [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,  $\mathbf{F}_p^a$ , 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 16. [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 113. [Frobenius mapping]** *mapping*

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

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

- $\varphi_{p,n}$  is (ring) homeomorphism with  $\text{Ker } \varphi_{p,n} = \{0\}$  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  $\mathbf{F}_{p^a}$ ,  $\mathbf{F}_{p^n}$  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 114. [fixed field]** for field,  $K$ , and group of automorphisms,  $G$ , of  $K$ ,

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

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 115. [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 116. [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  $G(K/k)$ ,  $G_{K/k}$ ,  $\text{Gal}(K/k)$ , or (simply)  $G$*

**Definition 117. [Galois group 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 group of polynomials and symmetric group]** *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*

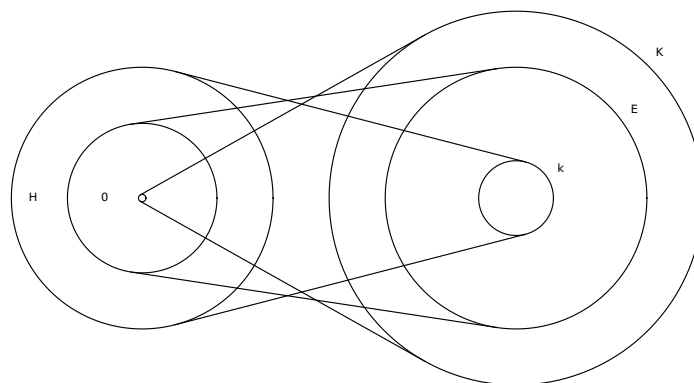
## Fundamental theorem for Galois theory

**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 the 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 12](#))*

**Definition 118. [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 17. [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  $F_1 F_2$ , i.e.,*

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

*(proof can be found in [Proof 13](#))*

**Corollary 18. [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 19. [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 14](#))*

**Corollary 20.** *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 17.** *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  $\text{Aut}(K)$  of order,  $n$ , and  $k = K^{\text{Aut}(K)}$ ,  $K/k$  is Galois,  $G(K/k) = \text{Aut}(K)$ , and  $[K : k] = n$

**Corollary 21. [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 21 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,  $\sigma$ , of set of all subgroups of  $G(K/k)$  into set of intermediate fields
  - $\sigma$  is *injective* since for any two subgroups,  $H$  and  $H'$ , of  $G(K/k)$ , if  $K^H = K^{H'}$ , then  $H = G(K/K^H) = G(K/K^{H'}) = H'$
  - $\sigma$  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,  $\sigma$  is isomorphism between set of all subgroups of  $G(K/k)$  and set of intermediate fields
  - since Theorem 28 implies separable extensions are distinguished,  $K/k$  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,  $G(K^H/k) \approx G(K/k)/H$

## Abelian and cyclic Galois extensions and groups

**Definition 119. [abelian Galois extensions]** *Galois extension with abelian Galois group, said to be abelian*

**Definition 120. [cyclic Galois extensions]** *Galois extension with cyclic Galois group, said to be cyclic*

**Corollary 22.** *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 121. [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

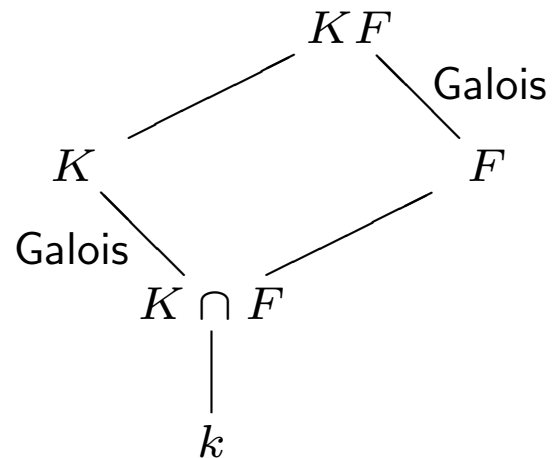
**Theorem 38.** *for Galois extension,  $K/k$ , and arbitrary extension,  $F/k$ , where  $K$  and  $F$  are subfields of common field,*

- $KF/F$  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 the figure*



**Corollary 23.** *for finite Galois extension,  $K/k$ , and arbitrary extension,  $F/k$ , where  $K$  and  $F$  are subfields of common field,*

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

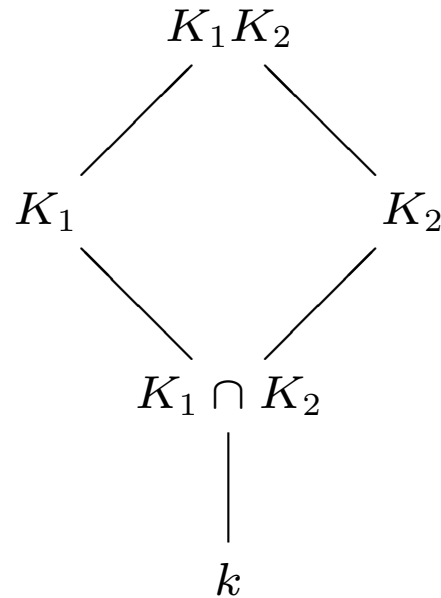
**Theorem 39.** *for Galois extensions,  $K_1/k$  and  $K_2/k$ , where  $K_1$  and  $K_2$  are subfields of common field,*

- $K_1K_2/k$  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 the figure*



**Corollary 24.** *for  $n$  Galois extensions,  $K_i/k$ , where  $K_1, \dots, K_n$  are subfields of common field and  $K_{i+1} \cap (K_1 \cdots K_i) = k$  for  $i = 1, \dots, n-1$ ,*

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

$$\sigma \mapsto (\sigma|_{K_1}, \dots, \sigma|_{K_n})$$

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



**Corollary 25.** *for Galois extension,  $K/k$ , where  $G(K/k)$  can be written as  $G_1 \times \cdots \times G_n$ , and  $K_1, \dots, K_n$ , each of which is fixed field of*

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

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

**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 122. [solvable 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 123. [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 117, 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), hence  $\mathbf{C}$  is algebraically closed*

# **Selected Proofs**

## Selected proofs

● **Proof 1.** (*Proof for “relation among coset indices” on page 20*)

Let  $\{h_1, \dots, h_n\}$  and  $\{k_1, \dots, k_m\}$  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  $1 \leq j, l \leq m$ ,  $h_i k_j K H = h_k k_l K H \Leftrightarrow h_i k_j H = h_k k_l H \Leftrightarrow h_i H = h_j H \Leftrightarrow h_i = h_j$ , 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

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

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

- For  $x, y \in G$ ,  $xG^CyG^C = xyG^C = G^Cxy = (G^Cx)(G^Cy)$ , hence  $G/G^C$  is commutative.
- For a homomorphism 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  $xyx^{-1}y^{-1} \in \text{Ker } f$ , hence  $G^C \subset \text{Ker } f$ .



● **Proof 3.** (*Proof for “set of functions into ring is ring” on page 56*)

- First, we show that the mapping addition defines a commutative additive group in  $\text{Map}(S, A)$ . The addition is associative because  $A$  is a ring, hence defines an

additive (abelian) group, thus, monoids (Definition 4 & Definition 5), *i.e.*,

$$\begin{aligned}
 & (\forall f, g, h \in \text{Map}(S, A)) \\
 & (\forall x \in S) ( ((f + g) + h)(x) = (f(x) + g(x)) + h(x) \\
 & \quad = f(x) + (g(x) + h(x)) = (f + (g + h))(x)) \\
 & \Rightarrow (f + g) + h = f + (g + h).
 \end{aligned}$$

Thus, the mapping addition defines an additive monoid in  $\text{Map}(S, A)$  with the zero mapping whose value is the additive unit element of  $A$  as the additive unit element of  $\text{Map}(S, A)$  (Definition 4). Now for every  $f \in R$ , a mapping  $g \in R$  defined by  $x \mapsto -f(x)$  satisfies  $f + g = g + f = 0$ , hence is the inverse of  $f$ . Therefore the additive monoid is a group (Definition 5). We further note that the addition is commutative because the additive group of  $A$  is abelian (Definition 36), *i.e.*,

$$\begin{aligned}
 & (\forall f, g \in S) \\
 & (\forall x \in M) ( (g + f)(x) = g(x) + f(x) = f(x) + g(x) = (f + g)(x)) \\
 & \Rightarrow f + g = g + f.
 \end{aligned}$$

Therefore, the mapping addition defines a commutative additive group in  $\text{End}(M)$ .

- The mapping multiplication is associative because  $A$  is ring, hence defines a multiplicative monoid, *i.e.*,

$$\begin{aligned}
 & (\forall f, g, h \in \text{Map}(S, A)) \\
 & (\forall x \in S) ( ((fg)h)(x) = (fg)(x)h(x) = (f(x)g(x))h(x) \\
 & \qquad \qquad = f(x)(g(x)h(x)) = f(x)(gh)(x) = (f(gh))(x)) \\
 & \Rightarrow \qquad (fg)h = f(gh).
 \end{aligned}$$

Thus, the mapping multiplication defines a multiplicative monoid in  $\text{Map}(S, A)$  with the mapping whose value is the multiplicative unit element of  $A$  as the multiplicative unit element (Definition 4).

- Now we show that the multiplication is distributive over addition in  $\text{Map}(S, A)$ . Similar this is due to that the multiplication is distributive over addition in  $A$ . Note



that

$$\begin{aligned}
 & (\forall f, g, h \in \text{Map}(S, A)) \\
 & (\forall x \in S) ( (f(g + h))(x) = f(x)(g + h)(x) = f(x)(g(x) + h(x)) \\
 & \quad = f(x)g(x) + f(x)h(x) = (fg)(x) + (fh)(x)) \\
 & \Rightarrow \quad f(g + h) = fg + fh.
 \end{aligned}$$

We can similarly show that

$$(\forall f, g, h \in \text{Map}(S, A)) ((f + g)h = fh + gh).$$

Therefore  $\text{Map}(S, A)$  is a ring (Definition 36). ■

- **Proof 4.** (*Proof for “set of group endomorphisms is ring” on page 56*)
  - First, we show that the addition defines a commutative additive group in  $\text{End}(M)$ .  
The addition is associative because  $M$  is a group, hence, monoids (Definition 4 &

Definition 5), *i.e.*,

$$\begin{aligned}
 & (\forall f, g, h \in \text{End}(M)) \\
 & \quad (\forall x \in M) \left( \begin{aligned} & ((f + g) + h)(x) = (f(x) + g(x)) + h(x) \\ & = f(x) + (g(x) + h(x)) = (f + (g + h))(x) \end{aligned} \right) \\
 & \Rightarrow \quad (f + g) + h = f + (g + h).
 \end{aligned}$$

Thus, the addition defines an additive monoid in  $\text{End}(M)$  with the zero mapping whose values is the unit element of  $M$  as the additive unit element (Definition 4). Now for every  $f \in \text{End}(M)$ , a mapping  $g \in \text{End}(M)$  defined by  $x \mapsto -f(x)$  satisfies  $f + g = g + f = 0$ , hence is the inverse of  $f$ . Therefore the addition defines the additive group in  $\text{End}(M)$  (Definition 5). We further note that the addition is commutative because  $M$  is abelian, *i.e.*,

$$\begin{aligned}
 & (\forall f, g \in \text{End}(M)) (\forall x \in M) \\
 & \quad ((g + f)(x) = g(x) + f(x) = f(x) + g(x) = (f + g)(x)).
 \end{aligned}$$

Therefore, the addition defines a commutative additive group in  $\text{End}(M)$ .

- The multiplication is associative because the mapping composition is an associative operation, *i.e.*,  $(\forall f, g, h \in \text{End}(M)) ((f \circ g) \circ h = f \circ (g \circ h))$ , hence, the mapping composition defines a multiplicative monoid in  $\text{End}(M)$  with the identity mapping as the multiplicative unit element (Definition 4).
- Now we show that the multiplication is distributive over addition. Note that

$$\begin{aligned}
 & (\forall f, g, h \in \text{End}(M)) \\
 & \quad (\forall x \in M) ( \quad (f \circ (g + h))(x) = f(g(x) + h(x)) \\
 & \qquad \qquad \qquad = (f \circ g)(x) + (f \circ h)(x)) \\
 & \Rightarrow \qquad \qquad f \circ (g + h) = (f \circ g) + (f \circ h).
 \end{aligned}$$

We can similarly show that

$$(\forall f, g, h \in \text{End}(M)) ((f + g) \circ h = (f \circ h) + (g \circ h)) .$$

Therefore for abelian group  $M$ , *set  $\text{End}(M)$  of group homeomorphisms of  $M$  into itself* is ring (Definition 36). ■

• **Proof 5.** (*Proof for “nonzero ideals of integers are principal” on page 62*)

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 (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 6.** (*Proof for “ideal generated by elements of ring” on page 64*)

For all  $x \in (a_1, \dots, a_n)$ , and  $y \in A$   $yx = y(\sum x_i a_i) = \sum (yx_i) a_i$  for some  $\langle x_i \rangle_{i=1}^n \subset A$ , hence  $yx \in A$ , and  $(a_1, \dots, a_n)$  is additive group, thus is ideal of  $A$ , hence

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

Conversely, if  $\mathfrak{a}$  contains  $a_1, \dots, a_n$ ,  $Aa_i \subset \mathfrak{a}$ , 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  $(a_1, \dots, a_n)$  is contained in

every ideal containing  $a_1, \dots, a_n$ , hence

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

■

- **Proof 7.** (*Proof for “kernel of ring-homeomorphism is ideal” on page 66*)

Let  $\text{Ker } f$  be the kernel of a ring homeomorphism  $f : A \rightarrow B$ . Then Definition 52 implies

$$(\forall a, b \in \text{Ker } f) (f(a + b) = f(a) + f(b) = 0 + 0 = 0 \Rightarrow a + b \in \text{Ker } f)$$

hence,  $\text{Ker } f$  is closed under addition. Also Definition 52 implies

$$(\forall a \in \text{Ker } f)$$

$$(f(-a) = f((-1)a) = f(-1)f(a) = f(-1)0 = 0 \Rightarrow -a \in \text{Ker } f)$$

hence, every element of  $\text{Ker } f$  has its inverse. Also  $0 \in \text{Ker } f$  because  $f(0) = 0$  by Definition 52. Thus,  $\text{Ker } f$  is a subgroup of  $A$  as additive group. Definition 52 also

implies

$$(\forall a \in A, x \in \text{Ker } f)$$

$$(f(ax) = f(a)f(x) = f(a)0 = 0 \ \& \ f(xa) = f(x)f(a) = 0f(a) = 0)$$

hence,  $\text{Ker } f$  is a two-side ideal, *i.e.*, an ideal. ■

● **Proof 8.** (*Proof for “image of ring-homeomorphism is subring” on page 70*)

Let  $f : A \rightarrow B$  be a ring-homeomorphism for two rings  $A$  and  $B$ .

- Then for any  $z, w \in f(A)$ , there exist  $x, y \in A$  such that  $f(x) = z$  and  $f(y) = w$ , hence Definition 52 implies

$$z + w = f(x) + f(y) = f(x + y) \in f(A)$$

because  $x + y \in A$ , hence  $f(A)$  is closed under addition. Because  $0 \in A$ , Definition 52 implies  $0 = f(0) \in f(A)$ , hence  $f(A)$  contains the additive unit element. Also, for every  $z \in f(A)$ , there exist  $x \in A$  such that  $f(x) = z$ , but there exists  $-x \in A$  because a ring is a commutative group with respect to addition

(Definition 36) thus,  $f(-x) \in f(A)$ , hence Definition 52 implies

$$f(-x) + z = f(-x) + f(x) = f(-x + x) = f(0) = 0$$

and the additive inverse of  $z$ , which is  $f(-x)$ , is in  $f(A)$ . Therefore  $f(A)$  is an additive group. Lastly for any  $z, w \in f(A)$ , there exist  $x, y \in A$  such that  $f(x) = z$  and  $f(y) = w$ , hence Definition 36 implies

$$z + w = f(x) + f(y) = f(x + y) = f(y + x) = f(y) + f(x) = w + z,$$

thus,

$$f(A) \subset B \text{ is a commutative group with respect to addition.} \quad (1)$$

- Then for any  $z, w \in f(A)$ , there exist  $x, y \in A$  such that  $f(x) = z$  and  $f(y) = w$ , hence Definition 52 implies

$$zw = f(x)f(y) = f(xy) \in f(A)$$

because  $xy \in A$ , hence  $f(A)$  is closed under multiplication. Because  $1 \in A$ , Definition 52 implies  $1 = f(1) \in f(A)$ , hence  $f(A)$  contains the multiplicative

unit element, thus,

$$f(A) \subset B \text{ is a monoid with respect to multiplication.} \quad (2)$$

Therefore  $f(A) \subset B$  is a subring of  $B$  by (1) and (2). ■

• **Proof 9.** (*Proof for “algebraicness of smallest subfields” on page 106*)

Proposition 25 implies that  $k(\alpha_1) = k[\alpha_1]$  and  $[k(\alpha_1) : k] = \deg \text{Irr}(\alpha_1, k, X)$ . Because  $\alpha_2$  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

$$[k(\alpha_1, \alpha_2) : k(\alpha_1)] = \deg \text{Irr}(\alpha_2, k(\alpha_1), X)$$

hence Proposition 23 implies

$$\begin{aligned} [k(\alpha_1, \alpha_2) : k] &= [k(\alpha_1, \alpha_2) : k(\alpha_1)][k(\alpha_1) : k] \\ &= \deg \text{Irr}(\alpha_1, k, X) \deg \text{Irr}(\alpha_2, k(\alpha_1), X). \end{aligned}$$



Using the mathematical induction, it is straightforward to show that

$$k(\alpha_1, \dots, \alpha_n) = k[\alpha_1, \dots, \alpha_n]$$

and

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

thus Proposition 22 implies that  $k(\alpha_1, \dots, \alpha_n)$  is finitely algebraic over  $k$ . ■

● **Proof 10.** (*Proof for “finite generation of compositum” on page 109*)

First, it is obvious that  $E = k(\alpha_1, \dots, \alpha_n) \subset F(\alpha_1, \dots, \alpha_n)$  and  $F \subset F(\alpha_1, \dots, \alpha_n)$ , hence  $EF \subset F(\alpha_1, \dots, \alpha_n)$  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  $f(\alpha_1, \dots, \alpha_n)$  where  $f \in F[X]$ , hence all  $f(\alpha_1, \dots, \alpha_n)/g(\alpha_1, \dots, \alpha_n)$  where  $f, g \in F[X]$  and  $g(\alpha_1, \dots, \alpha_n) \neq 0$ . Thus,  $F(\alpha_1, \dots, \alpha_n) \subset EF$  again by definition. Therefore  $EF = F(\alpha_1, \dots, \alpha_n)$ . ■

- **Proof 11.** (*Proof for “existence of algebraically closed algebraic extensions” on page 115*)

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  $\alpha$  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 12.** (*Proof for “theorem - Galois subgroups associated with intermediate fields” on page 136*)

Suppose  $\alpha \in K^G$  and let  $\sigma : k(\alpha) \rightarrow K^a$  be an embedding inducing the identity on  $k$ . If we let  $\tau : K \rightarrow K^a$  extend  $\sigma$ ,  $\tau$  is automorphism by normality of  $K/k$  (Definition 102), hence  $\tau \in G$ , thus  $\tau$  fixed  $\alpha$ , which means  $\sigma$  is the identity, which is the only embedding extension of the identity embedding of  $k$  onto itself to  $k(\alpha)$ , thus, by Definition 103,

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

Since  $K$  is separable over  $k$ ,  $\alpha$  is separable over  $k$  (by Theorem 26), and  $k(\alpha)$  is

separable over  $k$  (by Definition 105), 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 96). Thus,  $K/F$  is Galois (by Definition 115).

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 13.** (*Proof for “Galois subgroups associated with intermediate fields - 1” on page 136*)

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

$F_1 F_2$  fixed leaves both  $F_1$  and  $F_2$  fixed, hence  $G(K/F_1 F_2) \subset G(K/F_1) \cap G(K/F_2)$ . 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

$$(\forall n, m \in \mathbf{N})$$

$$(\forall x_1, \dots, x_n, x'_1, \dots, x'_m \in F_1, y_1, \dots, y_n, y'_1, \dots, y'_m \in F_2)$$

$$\left( \left( \frac{x_1 y_1 + \dots + x_n y_n}{x'_1 y'_1 + \dots + x'_m y'_m} \right)^\sigma = \frac{x_1 y_1 + \dots + x_n y_n}{x'_1 y'_1 + \dots + x'_m y'_m} \right) ,$$

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

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

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

- **Proof 14.** (*Proof for “Galois subgroups associated with intermediate fields - 3” on page 137*)

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  $\sigma \in G(K/F_2)$ . Since Theorem 35 implies that

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

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

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

■

# References

## References

- [DF99] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley and Sons, Inc., 2nd edition, 1999.
- [Lan93] Serge Lang. *Algebra*. Addison-Wesley Publishing Company, Inc., 3rd edition, 1993.



# Index

$G$ 

Galois group

finite extension, [133](#) $G$ -setgroup, [43](#) $G(K/k)$ 

Galois group

finite extension, [133](#) $G_{K/k}$ 

Galois group

finite extension, [133](#) $\text{Gal}(K/k)$ 

Galois group

finite extension, [133](#) $p$ -Sylow subgroups of finite groups, [49](#) $p$ -groupgroup, [49](#) $p$ -subgroupgroup, [49](#) $\mathbf{Z}/n\mathbf{Z}$ , [73](#)a fortiori algebraicness, [105](#)

a.e.

almost everywhere, [6](#)

a.s.

almost surely, [6](#)

Abel, Niels Henrik

abelian group, [14](#)abelian monoid, [13](#)abelian Galois extensions, [140](#)

abelian group, [14](#)

towers, [31](#)

abelian monoid, [13](#)

abstract algebra, [10](#)

history, [11](#)

why, [10](#)

action

group, [43](#)

addition

ring, [52](#)

algebraic

extension

dimension, [102](#)

over field, [99](#)

THE irreducible polynomial, [100](#)

algebraic and finite extensions are distinguished, [111](#)

algebraic closedness

field, [91](#)

algebraic closure, [117](#)

field, [117](#)

algebraic embedding extension

field, [116](#)

algebraic embedding extensions, [116](#)

algebraic extension, [96](#), [101](#)

field embeddings of, [113](#)

finite, [101](#)

Galois extension, [133](#)

algebraic over field, [99](#)

algebraically closed, [91](#)

field, [91](#)

algebraicness of finite field extensions, [101](#)

algebraicness of finitely generated subfield by single element, [105](#)

algebraicness of finitely generated subfields by multiple elements, [106](#)

almost everywhere, [6](#)

almost everywhere - a.e., [6](#)

almost surely, [6](#)

alternating group

finite symmetric group, [42](#)

alternating groups, [42](#)

arbitrary separable field extensions, [125](#)

Artin's theorem, [138](#)

associativity

group, [13](#)

automorphism

group, [16](#)

monoid, [16](#)

boundary

set, [3](#)

butterfly lemma

group, [36](#)

butterfly lemma - Zassenhaus, [36](#)

canonical isomorphisms

group, [27](#), [28](#)

canonical map

ring, [67](#)

canonical map of ring, [67](#)

canonical maps

group, [21](#)

cardinality of algebraic extension of infinite field,  
[117](#)

cardinality of algebraic extensions of infinite fields,  
[117](#)

center

of group, [22](#)

of ring, [53](#)

center of ring, [53](#)

centralizers

group, [22](#)

characteristic

field, [72](#)

ring, [71](#)

characteristic of ring, [71](#)

Chinese remainder theorem, [75](#)

class formula, [48](#)

group, [48](#)

closure

set, [3](#)

commutative group, [14](#)

commutative monoid, [13](#)

commutative ring, [53](#)

commutator, [34](#)  
group, [34](#)

commutator subgroup  
group, [34](#)

commutator subgroups, [34](#)

complement  
set, [2](#)

complex number, [2](#)

compositum  
field, [107](#)  
finite generation  
field, [109](#)

compositum of subfields, [107](#)

compositums

embedding, [113](#)  
field, [113](#)

compositums of fields, [113](#)

congruence with respect to normal subgroup, [23](#)  
group, [23](#)

conjugate  
group, [44](#)

conjugates of elements of fields, [126](#)

conjugates of fields, [126](#)

conjugation  
group, [44](#)

conjugation of groups, [44](#)

constant and monic polynomials, [86](#)

constant polynomial, [86](#)

convolution product, [59](#)  
ring, [59](#)

corollaries

existence of algebraically closed algebraic field  
extensions, [115](#)

existence of extension fields containing roots,  
[115](#)

factoriality of polynomial ring, [85](#)

finite dimension of extension, [102](#)

finite field extensions, [128](#)

Galois subgroups associated with intermediate  
fields - 1, [136](#)

Galois subgroups associated with intermediate  
fields - 2, [137](#)

Galois subgroups associated with intermediate  
fields - 3, [137](#)

Galois subgroups associated with intermediate  
fields - 4, [138](#)

induction of zero function in multiple variables,  
[88](#)

induction of zero function in one variable, [88](#)

induction of zero functions in multiple variables  
- finite fields, [88](#)

induction of zero functions in multiple variables  
- infinite fields, [88](#)

isomorphism between algebraically closed  
algebraic extensions, [116](#)

isomorphism between splitting fields for family  
of polynomials, [119](#)

isomorphism induced by Chinese remainder  
theorem, [75](#)

multiplicative subgroup of finite field is cyclic,  
[90](#)

uniqueness of reduced polynomials, [89](#)

coset

group, [19](#)

coset representation

group, [19](#)

cosets of groups, [19](#)

countability of algebraic closure of finite field, [117](#)

countability of algebraic closure of finite fields, [117](#)

cyclic Galois extensions, [140](#)

cyclic generator

group, [15](#)

cyclic group

towers, [31](#)

cyclic groups, [15](#)

definitions

abelian Galois extensions, [140](#)

algebraic closure, [117](#)

algebraic extension, [101](#)

algebraic over field, [99](#)

algebraically closed, [91](#)

almost everywhere - a.e., [6](#)

alternating groups, [42](#)

arbitrary separable field extensions, [125](#)

canonical map of ring, [67](#)

center of ring, [53](#)

characteristic of ring, [71](#)

commutative ring, [53](#)

commutator, [34](#)

commutator subgroups, [34](#)

compositum of subfields, [107](#)



congruence with respect to normal subgroup, [23](#)

conjugates of elements of fields, [126](#)

conjugates of fields, [126](#)

conjugation of groups, [44](#)

constant and monic polynomials, [86](#)

convolution product, [59](#)

cosets of groups, [19](#)

cyclic Galois extensions, [140](#)

cyclic groups, [15](#)

derivative of polynomial over commutative ring, [92](#)

devision of entire ring elements, [78](#)

dimension of extension, [102](#)

direct products, [15](#)

distinguished class of field extensions, [110](#)

division ring, [53](#)

embedding of homeomorphism, [17](#)

embedding of ring, [70](#)

entire ring, [65](#)

equivalent towers, [38](#)

Euler phi-function, [74](#)

evaluation homeomorphism, [82](#)

exact sequences of homeomorphisms, [24](#)

exponent of groups and group elements, [40](#)

extension of field, [98](#)

factor ring and residue class, [67](#)

factorial ring, [77](#)

field, [54](#)

field embedding, [112](#)

field embedding extension, [112](#)

finite fields, [128](#)

finite separable field extensions, [124](#)

finite tower of fields, [104](#)

fixed field, [132](#)

Frobenius endomorphism, [94](#)  
Frobenius mapping, [129](#)  
Galois extensions, [133](#)  
Galois group of polynomials, [133](#)  
Galois groups, [133](#)  
Galois subgroups associated with intermediate fields, [136](#)  
generation of field extensions, [103](#)  
generators, [15](#)  
generators of ideal, [64](#)  
greatest common divisor, [78](#)  
group, [14](#)  
group ring, [58](#)  
homeomorphism, [16](#)  
ideal, [61](#)  
index and order of group, [19](#)  
induced injective ring-homeomorphism, [70](#)

infinitely often - i.o., [6](#)  
irreducible polynomials, [86](#)  
irreducible ring element, [77](#)  
isotropy, [46](#)  
kernel of homeomorphism, [17](#)  
law of composition, [13](#)  
lifting, [108](#)  
maximal ideal, [69](#)  
maximum abelian extension, [140](#)  
monoids, [13](#)  
multiplicative group of invertible elements of ring, [53](#)  
multiplicative subgroup of field, [90](#)  
multiplicity and multiple roots, [93](#)  
normal extensions, [120](#)  
normal subgroups, [21](#)  
normalizers and centralizers, [22](#)

operations of group on set, [43](#)  
orbits of operation, [47](#)  
period of group elements, [40](#)  
polynomial, [81](#)  
polynomial function, [82](#)  
prime field, [72](#)  
prime ideal, [69](#)  
prime ring, [72](#)  
primitive  $n$ -th root of unity, [90](#)  
primitive element of fields, [127](#)  
principal ideal, [61](#)  
principal ring, [62](#)  
principal two-sided ideal, [61](#)  
reduced polynomials, [89](#)  
reduction map, [84](#)  
reduction of  $f$  modulo  $p$ , [84](#)  
refinement of towers, [33](#)

ring, [52](#)  
ring of integers modulo  $n$ , [73](#)  
ring-homeomorphism, [66](#)  
ring-isomorphism, [70](#)  
root of polynomial, [87](#)  
separable algebraic elements, [124](#)  
separable closure, [126](#)  
separable degree of field extensions, [122](#)  
separable polynomials, [124](#)  
simple groups, [35](#)  
solvable by radicals, [145](#)  
solvable groups, [33](#)  
solvable extensions, [145](#)  
splitting fields, [118](#)  
splitting fields for family of polynomials, [119](#)  
subring, [52](#)  
sylow subgroups, [49](#)

symmetric groups and permutations, [42](#)

THE irreducible polynomial, [100](#)

tower of fields, [104](#)

towers of groups, [31](#)

transitive operation, [47](#)

translation, [45](#)

unique factorization into irreducible elements,  
[77](#)

variables and transcendental, [82](#)

zero divisor, [65](#)

derivative

of polynomial, [93](#)

polynomial, [92](#)

derivative of polynomial, [93](#)

derivative of polynomial over commutative ring, [92](#)

division of entire ring elements, [78](#)

difference

set, [3](#)

dimension

algebraic extension, [102](#)

field

algebraic extension, [102](#)

dimension of extension, [102](#)

dimension of finite extension, [102](#)

direct products, [15](#)

group, [15](#)

distinguished class

field

extension, [110](#)

distinguished class of field extensions, [110](#)

division ring, [53](#)

embedding

extension

field, [112](#)

field, [112](#)

group homeomorphism, [17](#)

ring, [70](#)

embedding of homeomorphism, [17](#)

embedding of ring, [70](#)

embeddings of compositum of fields, [113](#)

endomorphism

group, [16](#)

monoid, [16](#)

entire ring, [65](#)

integral domain, [65](#)

equivalent towers, [38](#)

group, [38](#)

Euclidean algorithm, [85](#)

polynomial ring, [85](#)

Euler  $\varphi$ -function, [74](#)

Euler phi-function, [74](#)

Euler's theorem, [74](#)

Euler's totient function, [74](#)

Euler, Leonhard

$\varphi$ -function, [74](#)

Euler's theorem, [74](#)

Euler's totient function, [74](#)

phi-function, [74](#)

evaluation homeomorphism, [82](#)

even

finite symmetric group, [42](#)

every field is entire ring, [65](#)

exact sequences of homeomorphisms, [24](#)

group, [24](#)

existence of algebraically closed algebraic field extensions, [115](#)

existence of algebraically closed field extensions, [115](#)

existence of extension fields containing roots, [115](#)

existence of greatest common divisor of principal entire rings, [78](#)

existence of roots of irreducible polynomial, [114](#)

exponent

group, [40](#)

exponent of groups and group elements, [40](#)

extension

algebraic, [101](#)

finite, [101](#)

field, [98](#)

finite, [98](#)

infinite, [98](#)

extension of field, [98](#)

extensions solvable by radicals, [145](#)

factor group

group, [21](#)

factor ring

ring, [67](#)

factor ring and residue class, [67](#)

factor ring induced ring-homeomorphism, [68](#)

factorial ring, [77](#)

factoriality of polynomial ring, [85](#)

Feit, Walter

Feit-Thompson theorem, [33](#)

Feit-Thompson theorem, [33](#)

field, [54](#)

a fortiori algebraicness, [105](#)

algebraic closedness, [91](#)

algebraic closure, [117](#)

algebraic embedding extension, [116](#)

algebraic extension, [96](#), [97](#), [101](#)

distinguished, [111](#)

finite, [101](#)

algebraic over field, [99](#)

algebraically closed extension, [91](#)

algebraicness

a fortiori, [105](#)

finitely generated subfield by multiple elements, [106](#)

finitely generated subfield by single element, [105](#)

cardinality of algebraic extension of infinite field, [117](#)

characteristic, [72](#)

compositum, [107](#)

finite generation, [109](#)

compositums, [113](#)

countability of algebraic closure of finite field, [117](#)

- dimension
  - extension, [102](#)
- dimension of extension
  - finiteness, [102](#)
- dimension of finite extension, [102](#)
- embedding, [112](#)
  - compositums, [113](#)
  - extension, [112](#)
- existence of algebraically closed algebraic extension, [115](#)
- existence of algebraically closed extensions, [115](#)
- existence of extension fields containing roots, [115](#)
- extension, [98](#)
  - algebraic, [101](#)
  - algebraically closed algebraic, [115](#)
  - distinguished class, [110](#)
  - finite, [98](#), [103](#)
  - finitely generated, [103](#)
  - generation, [103](#)
  - infinite, [98](#)
- extension of field, [98](#)
- finite extension
  - distinguished, [111](#)
- finite tower of fields, [104](#)
- fixed field, [132](#)
- generation of extension, [103](#)
- having characteristic  $p$ , [94](#), [95](#)
- isomorphic image of  $\mathbf{Q}$  or  $\mathbf{F}_p$ , [72](#)
- isomorphism between algebraically closed algebraic extensions, [116](#)
- lifting, [108](#)
- multiplicative subgroup of field, [90](#)
- number of algebraic embedding extensions, [116](#)
- prime, [72](#), [73](#)



splitting, [118](#)

isomorphism, [118](#)

THE irreducible polynomial, [100](#)

tower of fields, [104](#)

translation, [108](#)

field embedding, [112](#)

of algebraic extension, [113](#)

field embedding extension, [112](#)

field embedding of algebraic extension, [113](#)

field homeomorphism, [66](#)

injectivity, [66](#)

finite dimension of extension, [102](#)

finite extension is finitely generated, [103](#)

finite field extensions, [128](#)

finite fields, [128](#)

finite generation of compositum, [109](#)

finite group, [14](#)

finite multiplicative subgroup of field is cyclic, [90](#)

finite separable field extensions, [124](#)

finite sequence, [2](#)

finite solvable groups, [33](#)

finite tower of fields, [104](#)

fixed field, [132](#)

fixed points

group

operation, [46](#)

formula

class formula, [48](#)

orbit decomposition formula, [48](#)

Frobenius endomorphism, [94](#)

polynomial, [94](#)

Frobenius mapping, [129](#)

Frobenius, Ferdinand Georg

Frobenius endomorphism

polynomial, [94](#)

fundamental theorem

for Galois theory, [134](#)

of algebra, [146](#)

fundamental theorem for Galois theory, [134](#)

fundamental theorem of algebra, [146](#)

Galois extension

algebraic extension, [133](#)

Galois extensions, [133](#)

Galois group of polynomials, [133](#)

Galois group of polynomials and symmetric group,  
[133](#)

Galois groups, [133](#)

Galois subgroups associated with intermediate  
fields, [136](#)

Galois subgroups associated with intermediate fields  
- 1, [136](#)

Galois subgroups associated with intermediate fields  
- 2, [137](#), [138](#)

Galois subgroups associated with intermediate fields  
- 3, [137](#)

Galois subgroups associated with intermediate fields  
- 4, [138](#)

Galois theory, [130](#), [131](#), [134](#)  
    appreciation, [131](#)

Galois, Évariste  
    Galois extension, [133](#)  
    Galois group, [133](#)  
    Galois theory, [134](#)

generated by  
    ring  
        ideal, [64](#)

generation of field extensions, [103](#)

generators, [15](#)  
    group, [15](#)

generators of ideal, [64](#)

of ring, [64](#)

greatest common divisor, [78](#)  
    principal entire ring, [78](#)  
    ring, [78](#)

group, [14](#)  
     $G$ -set, [43](#)  
     $p$ -group, [49](#)  
     $p$ -subgroup, [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 subgroup, [34](#)  
congruence with respect to normal subgroup, [23](#)  
  
conjugate, [44](#)  
conjugation, [44](#)  
coset, [19](#)  
coset representation, [19](#)  
cyclic, [15](#)  
cyclic generator, [15](#)  
cyclic group, [15](#)  
direct products, [15](#)  
endomorphism, [16](#)  
equivalent towers, [38](#)

exact sequences of homeomorphisms, [24](#)  
exponent, [40](#)  
factor group, [21](#)  
finite, [14](#)  
Galois group, [133](#)  
generators, [15](#)  
homeomorphism, [16](#)  
    injective, [17](#)  
index, [19](#)  
inner, [44](#)  
isomorphism, [16](#)  
isotropy, [46](#)  
Jordan-Hölder theorem, [39](#)  
law of composition, [13](#)  
left coset, [19](#)  
monoid, [13](#)  
normal subgroup, [21](#)

- normalizers, [22](#)
- operation, [43](#)
  - faithful, [46](#)
  - fixed points, [46](#)
  - orbits, [47](#)
  - transitive, [47](#)
- orbit decomposition formula, [48](#)
- order, [19](#)
- orthogonal subgroup, [18](#)
- period
  - elements, [40](#)
- permutations, [42](#)
- refinement of towers, [33](#)
- right coset, [19](#)
- Schreier theorem, [39](#)
- simple, [35](#)
- solvable group, [33](#)

- special linear group, [22](#)
- syLOW subgroup, [49](#)
- symmetric, [42](#)
  - alternating, [42](#)
  - even, [42](#)
  - odd, [42](#)
- towers, [31](#)
  - abelian, [31](#)
  - cyclic, [31](#)
  - equivalent, [38](#)
  - normal, [31](#)
- translation, [45](#)
- unit element, [13](#)

group homeomorphism and isomorphism, [17](#)

group of automorphisms of finite fields, [129](#)

group of automorphisms of finite fields over another finite field, [129](#)

group of invertible elements

ring, [53](#)

group of units

ring, [53](#)

group ring, [58](#)

ring, [58](#)

Hölder, Ludwig Otto

Jordan-Hölder theorem, [39](#)

homeomorphism, [16](#)

group, [16](#)

embedding, [17](#)

injective, [17](#)

kernel, [17](#)

monoid, [16](#)

ring-homeomorphism, [66](#)

sign homeomorphism

of finite symmetric group, [42](#)

i.o.

infinitely often, [6](#)

ideal, [61](#)

of ring, [61](#)

generators of, [64](#)

left, [61](#)

maximal, [69](#)

prime, [69](#)

right, [61](#)

two-sided, [61](#)

ideals of field, [61](#)

image of ring-homeomorphism is subring, [70](#)

index

group, [19](#)

index and order of group, [19](#)

indices and orders, [20](#)

induced injective ring-homeomorphism, [70](#)

induction of zero function in multiple variables, [88](#)

induction of zero function in one variable, [88](#)

induction of zero functions in multiple variables -  
finite fields, [88](#)

induction of zero functions in multiple variables -  
infinite fields, [88](#)

infinite sequence, [2](#)

infinitely often, [6](#)

infinitely often - i.o., [6](#)

injective

homeomorphism

group, [17](#)

injectivity of field homeomorphism, [66](#)

inner

group, [44](#)

insolvability of quintic polynomials, [146](#)

integer, [2](#)

integral domain, [65](#)

interior

set, [3](#)

inverse

group, [14](#)

irreducible element

ring

entire, [77](#)

irreducible polynomial, [86](#)

existence of roots, [114](#)

irreducible polynomials, [86](#)

irreducible ring element, [77](#)

isomorphism

group, [16](#)

monoid, [16](#)

isomorphism between algebraically closed algebraic  
extensions, [116](#)

field, [116](#)

isomorphism between splitting fields, [118](#)

isomorphism between splitting fields for family of  
polynomials, [119](#)

isomorphism induced by Chinese remainder  
theorem, [75](#)

isomorphism of endomorphisms of cyclic groups, [76](#)

isotropy, [46](#)

group, [46](#)

Jordan, Marie Ennemond Camile

Jordan-Hölder theorem, [39](#)

Jordan-Hölder theorem, [39](#)

kernel

group homeomorphism, [17](#)

ring-homeomorphism, [66](#)

kernel of homeomorphism, [17](#)



law of composition, [13](#)

group, [13](#)

left coset

group, [19](#)

left ideal

of ring, [61](#)

lemmas

a fortiori algebraicity, [105](#)

butterfly lemma - Zassenhaus, [36](#)

compositums of fields, [113](#)

embeddings of compositum of fields, [113](#)

every field is entire ring, [65](#)

existence of roots of irreducible polynomial, [114](#)

field embedding of algebraic extension, [113](#)

finite generation of compositum, [109](#)

ideals of field, [61](#)

image of ring-homeomorphism is subring, [70](#)

normality of subgroups of order  $p$ , [50](#)

number of fixed points of group operations, [49](#)

properties of prime and maximal ideals, [69](#)

lifting, [108](#)

field, [108](#)

matrix

positive definite, [4](#)

positive semi-definite, [4](#)

symmetric, [4](#)

trace, [3](#)

maximal ideal, [69](#)

of ring, [69](#)

properties, [69](#)

maximum abelian extension, [140](#)

modulo

ring of integers modulo  $n$ , [73](#)

monic polynomial, [86](#)

monoid

abelian, [13](#)

automorphism, [16](#)

commutative, [13](#)

endomorphism, [16](#)

group, [13](#)

homeomorphism, [16](#)

isomorphism, [16](#)

monoid-homeomorphism, [16](#)

monoids, [13](#)

multiple roots

necessary and sufficient condition for multiple roots

polynomial, [93](#)

polynomial, [93](#)

multiplication

ring, [52](#)

multiplicative group of finite field, [128](#)

multiplicative group of invertible elements of ring, [53](#)

multiplicative subgroup of field, [90](#)

multiplicative subgroup of finite field is cyclic, [90](#)

multiplicativity of separable degree of field extensions, [123](#)

multiplicity

polynomial, [93](#)

multiplicity and multiple roots, [93](#)

mylemma, [61](#)

natural number, [2](#)

necessary and sufficient condition for multiple roots,  
[93](#)

norm

vector, [3](#)

normal extensions, [120](#)

normal group

towers, [31](#)

normal subgroup

group, [21](#)

normal subgroups, [21](#)

normal subgroups and factor groups, [21](#)

normality of subgroups of order  $p$ , [50](#)

normalizers

group, [22](#)

normalizers and centralizers, [22](#)

normalizers of groups, [23](#)

number

complex number, [2](#)

integer, [2](#)

natural number, [2](#)

rational number, [2](#)

real number, [2](#)

number of algebraic embedding extensions, [116](#)

field, [116](#)

number of fixed points of group operations, [49](#)

number of roots of polynomial, [87](#)

odd

finite symmetric group, [42](#)

operation

group, [43](#)

faithful, [46](#)

fixed points, [46](#)

orbits, [47](#)

transitive, [47](#)

operations of group on set, [43](#)

orbit decomposition formula, [48](#)

group, [48](#)

orbits

group

operation, [47](#)

orbits of operation, [47](#)

order

group, [19](#)

orthogonal subgroup

group, [18](#)

orthogonal subgroups, [18](#)

period

group

elements, [40](#)

period of elements of finite groups, [40](#)

period of group elements, [40](#)

permutations

group, [42](#)

transposition, [42](#)

polynomial ring

polynomial function, [82](#)

polynomial, [79](#), [81](#)

algebraically closed, [91](#)

constant, [86](#)

derivative, [92](#), [93](#)

Frobenius endomorphisms, [94](#)

induction of zero function

in multiple variables, [88](#)

induction of zero function in multiple variables,  
[88](#)

finite field, [88](#)

induction of zero function in one variable, [88](#)

irreducible, [86](#)

monic, [86](#)

multiple roots, [93](#)

necessary and sufficient condition for multiple  
roots, [93](#)

multiplicity, [93](#)

over arbitrary commutative ring, [80](#)

over field field, [80](#)

polynomial ring, [81](#)

primitive  $n$ -th roots of unity, [90](#)

reduced, [89](#)

ring, [80](#)

root, [87](#)

root of polynomial, [87](#)

with integer coefficients, [80](#)

zero, [87](#)

polynomial function, [82](#)

## polynomial ring

- Euclidean algorithm, [85](#)
- evaluation homeomorphism, [82](#)
- factoriality, [85](#)
- irreducible polynomial, [86](#)
- polynomial, [81](#)
- principality, [85](#)
- reduction map, [84](#)
- reduction of  $f$  modulo  $p$ , [84](#)
- ring, [80](#)
- substitution homeomorphism, [82](#)
- transcendental, [82](#)
- variable, [82](#)

positive definite matrix, [4](#)

positive semi-definite matrix, [4](#)

prime

field, [73](#)

prime element theorem, [127](#)

prime field, [72](#)

prime ideal, [69](#)

- of ring, [69](#)
- properties, [69](#)

prime ring, [72](#)

primitive  $n$ -th root of unity, [90](#)

- polynomial, [90](#)

primitive element of fields, [127](#)

principal entire ring is factorial, [78](#)

principal ideal, [61](#)

principal ring, [62](#)

principal two-sided ideal, [61](#)

principality of polynomial ring, [85](#)

properties of cyclic groups, [41](#)

properties of prime and maximal ideals, [69](#)

propositions

algebraic and finite extensions are distinguished, [111](#)

algebraicness of finite field extensions, [101](#)

algebraicness of finitely generated subfield by single element, [105](#)

algebraicness of finitely generated subfields by multiple elements, [106](#)

cosets of groups, [19](#)

derivative of polynomial, [93](#)

dimension of finite extension, [102](#)

existence of extension fields containing roots, [115](#)

existence of greatest common divisor of principal entire rings, [78](#)

factor ring induced ring-homeomorphism, [68](#)

finite extension is finitely generated, [103](#)

finite solvable groups, [33](#)

Galois group of polynomials and symmetric group, [133](#)

group homeomorphism and isomorphism, [17](#)

indices and orders, [20](#)

injectivity of field homeomorphism, [66](#)

necessary and sufficient condition for multiple roots, [93](#)

normal subgroups and factor groups, [21](#)

normalizers of groups, [23](#)

number of algebraic embedding extensions, [116](#)

orthogonal subgroups, [18](#)

period of elements of finite groups, [40](#)

properties of cyclic groups, [41](#)

separability and multiple roots, [124](#)  
sign homeomorphism of finite symmetric groups,  
[42](#)  
simple groups, [35](#)  
solvability of groups of order  $pq$ , [50](#)  
subgroups of cyclic groups, [40](#)  
towers inded by homeomorphism, [31](#)

rational number, [2](#)

real number, [2](#)

reduced polynomial  
uniqueness, [89](#)

reduced polynomials, [89](#)

reduction map, [84](#)  
polynomial ring, [84](#)  
reduction of  $f$  modulo  $p$ , [84](#)

ring, [84](#)

reduction of  $f$  modulo  $p$ , [84](#)

refinement of towers, [33](#)  
group, [33](#)

relative interior  
set, [3](#)

residue class  
ring, [67](#)

retention of normality of extensions, [121](#)

right coset  
group, [19](#)

right ideal  
of ring, [61](#)



ring, [52](#)

addition, [52](#)

canonical map, [67](#)

center of, [53](#)

characteristic, [71](#)

Chinese remainder theorem, [75](#)

isomorphism induced by, [75](#)

commutative, [53](#)

convolution product, [59](#)

devision of elements, [78](#)

division ring, [53](#)

embedding, [70](#)

entire, [65](#)

devision of elements, [78](#)

factorial, [77](#)

irreducible element, [77](#)

unique factorization, [77](#)

factor ring, [67](#)

factor ring induced ring-homeomorphism, [68](#)

factorial, [77](#)

generated by ideal, [64](#)

generators of ideal, [64](#)

greatest common divisor, [78](#)

greatest common divisor of principal entire ring,  
[78](#)

group of invertible elements, [53](#)

group of units, [53](#)

group ring, [58](#)

ideal, [61](#)

left ideal, [61](#)

maximal, [69](#)

prime, [69](#)

right ideal, [61](#)

two-sided ideal, [61](#)

induced injective ring-homeomorphism, [70](#)

integer, [73](#)

isomorphism induced by Chinese remainder theorem, [75](#)

isomorphism of endomorphisms of cyclic groups, [76](#)

maximal ideal, [69](#)

properties, [69](#)

multiplication, [52](#)

multiplicative group of invertible elements of ring, [53](#)

of integers modulo  $n$ , [73](#)

prime, [73](#)

of polynomial differential operators, [80](#)

polynomial, [80](#), [81](#)

polynomial ring, [80](#)

prime, [72](#)

prime ideal, [69](#)

properties, [69](#)

principal, [62](#)

principal ideal, [61](#)

principal two-sided ideal, [61](#)

reduction map, [84](#)

residue class, [67](#)

ring-homeomorphism, [66](#)

kernel, [66](#)

subring, [52](#)

units, [53](#)

zero divisor, [65](#)

ring homeomorphism

field homeomorphism, [66](#)

ring of integers modulo  $n$ , [73](#)

ring-homeomorphism, [66](#)

kernel, [66](#)

ring-isomorphism, [70](#)

root

polynomial, [87](#)

root of polynomial, [87](#)

Schreier theorem, [39](#)

group, [39](#)

Schreier, Otto

Schreier theorem, [39](#)

separability and multiple roots, [124](#)

separable algebraic elements, [124](#)

separable closure, [126](#)

separable degree of field extensions, [122](#)

separable extensions are distinguished, [125](#)

separable field extensions, [125](#)

separable polynomials, [124](#)

sequence, [2](#)

finite sequence, [2](#)

infinite sequence, [2](#)

set

boundary, [3](#)

closure, [3](#)

complement, [2](#)

difference, [3](#)

interior, [3](#)

relative interior, [3](#)

sign homeomorphism

of finite symmetric group, [42](#)

sign homeomorphism of finite symmetric groups, [42](#)

simple groups, [35](#)

simplicity of alternating groups, [42](#)

smallest  $\sigma$ -algebra containing subsets, [3](#)

solvability condition in terms of normal subgroups, [33](#)

solvability of finite  $p$ -groups, [50](#)

solvability of finite symmetric groups, [42](#)

solvability of groups of order  $pq$ , [50](#)

solvable by radicals, [145](#)

solvable extensions are distinguished, [145](#)

solvable group  
group, [33](#)

solvable groups, [33](#)

solvable extensions, [145](#)

special linear group  
group, [22](#)

splitting field, [118](#)  
isomorphism, [118](#)

splitting fields, [118](#)

splitting fields for family of polynomials, [119](#)

subgroup, [14](#)  
group, [14](#)  
trivial, [14](#)

subgroups of cyclic groups, [40](#)

submonoid, [13](#)  
monoid, [13](#)

subring, [52](#)

ring, [52](#)

syLOW subgroup

group, [49](#)

syLOW subgroups, [49](#)

symmetric group

group, [42](#)

transposition, [42](#)

symmetric groups and permutations, [42](#)

symmetric matrix, [4](#)

THE irreducible polynomial, [100](#)

theorems

$p$ -Sylow subgroups of finite groups, [49](#)

algebraic embedding extensions, [116](#)

Artin's theorem, [138](#)

cardinality of algebraic extensions of infinite fields, [117](#)

Chinese remainder theorem, [75](#)

countability of algebraic closure of finite fields, [117](#)

Euclidean algorithm, [85](#)

Euler's theorem, [74](#)

existence of algebraically closed field extensions, [115](#)

extensions solvable by radicals, [145](#)

Feit-Thompson theorem, [33](#)

finite fields, [128](#)

finite multiplicative subgroup of field is cyclic, [90](#)

finite separable field extensions, [124](#)

fundamental theorem for Galois theory, [134](#)

fundamental theorem of algebra, [146](#)

Galois subgroups associated with intermediate fields - 1, [136](#)

Galois subgroups associated with intermediate fields - 2, [138](#)

group of automorphisms of finite fields, [129](#)

group of automorphisms of finite fields over another finite field, [129](#)

insolvability of quintic polynomials, [146](#)

isomorphism between splitting fields, [118](#)

isomorphism of endomorphisms of cyclic groups, [76](#)

multiplicative group of finite field, [128](#)

multiplicativity of separable degree of field extensions, [123](#)

normal extensions, [120](#)

number of roots of polynomial, [87](#)

prime element theorem, [127](#)

principal entire ring is factorial, [78](#)

principality of polynomial ring, [85](#)

retention of normality of extensions, [121](#)

Schreier theorem, [39](#)

separable extensions are distinguished, [125](#)

separable field extensions, [125](#)

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, [145](#)

upper limit on separable degree of field extensions, [123](#)

Thompson, John Griggs

Feit-Thompson theorem, [33](#)

tower of fields, [104](#)

towers

abelian, [31](#)

cyclic, [31](#)

equivalent, [38](#)

group, [31](#)

inded by homeomorphism, [31](#)

normal, [31](#)

refinement, [33](#)

towers inded by homeomorphism, [31](#)

towers of groups, [31](#)

trace

matrix, [3](#)

transitive

group

operation, [47](#)

transitive operation, [47](#)

translation, [45](#)

field, [108](#)

group, [45](#)

transpositions

permutations, [42](#)

symmetric group, [42](#)

trivial subgroup, [14](#)

two-sided ideal

of ring, [61](#)

unique factorization

ring

entire, [77](#)

unique factorization into irreducible elements, [77](#)

uniqueness of reduced polynomials, [89](#)

unit element

group, [13](#)

units

ring, [53](#)

upper limit on separable degree of field extensions,  
[123](#)

variables and transcendental, [82](#)

vector

norm, [3](#)

vector space

as field extension, [98](#)

Zassenhaus, Hans

butterfly lemma, [36](#)

zero

polynomial, [87](#)

zero divisor, [65](#)

ring, [65](#)

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, [141](#)

diagram for Galois two-side lifting, [143](#)

diagrams for Galois main result, [135](#)

embedding extension, [112](#)

factor-ring-induced-ring-homeomorphism, [68](#)



lattice diagram of fields, [110](#)

lifting or smallest fields, [109](#)

translation or lifting of fields, [108](#)

### ZZ-important

for field  $k$  and its algebraic extension  $E$ ,  
embedding of  $E$  into itself over  $k$  is  
isomorphism, [113](#)

algebraically closed algebraic extension is  
determined up to isomorphism, [116](#)

group having an abelian tower whose last  
element is trivial subgroup, said to be  
[solvable](#), [33](#)

### ZZ-todo

0 - apply new comma conventions, [0](#)

1 - convert bullet points to proper theorem,  
definition, lemma, corollary, proposition, etc.,  
[0](#)

CANCELED - < 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](#)

DONE - 2025 0414 - 1 - change mathematicians’  
names, [0](#)