Author: kiking

Chapter 1 Why Abstract Algebra?

Italian Renaissance, 16th century algebra

Problem-solving Competitions

Girolamo Cardan (1501), Book Ars Magna (The Great Art)

Tartaglia (~1500) - solving any cubic equation $x^3+ax^2+bx=c$

Ludovico Ferrari - solving any quadratic equations $x^4+ax^3+bx^2+cx=d$

1824, Niels Abel (Norwegian) = ∄ formulas for roots for degree ≥ 5

Similar times = Matrix Algebra

Boolean Algebra

⋮

Axiomatics / Abstraction = varying the possible choices of axioms

1845, Évariste Galois = explains exactly which equations of degree ≥ 5 have solutions (traditional kind), which do not

(published) (1832 died)

~1930, Early 20th Centuries = Algebraic Structure (completed)

Chapter 2 Operations

Valid operations on a set A.

① $a * b$ is defined for every ordered pair $(a,b) \in A$

② $a * b$ uniquely defined

③ $a * b \in A$

Exercises

B. Properties of Operations

7. $x * y = \dfrac{xy}{x+y+1}$

(a) commutative ?

Author: kiking

$$y*x = \frac{yx}{y+x+1} = x*y \longrightarrow \text{is commutative}$$

(b) associative ?

$$x*(y*z) = \frac{x\left(\frac{yz}{y+z+1}\right)}{x+\left(\frac{yz}{y+z+1}\right)+1} = \frac{xyz}{y+z+1}\cdot\frac{y+z+1}{x(y+z+1)+yz+(y+z+1)}$$

$$= \frac{xyz}{(x+1)(y+z+1)+yz} = \frac{xyz}{xy+xz+yz+x+y+z}$$

$$(x*y)*z = \frac{\left(\frac{xy}{x+y+1}\right)\cdot z}{\left(\frac{xy}{x+y+1}\right)+z+1} = \frac{xyz}{x+y+1}\cdot\frac{x+y+1}{xy+z(x+y+1)+(x+y+1)}$$

$$= \frac{xyz}{(z+1)(x+y+1)+xy} = \frac{xyz}{xy+xz+yz+x+y+z}$$

$\Big\}$ is associative

(c) has an identity ? (on $\mathbb{R}^+$)

$$x*e = \frac{xe}{x+e+1} = x$$

$$xe = x(x+e+1)$$

$x = 0$ or $-1 \notin \mathbb{R}^+$ $\longrightarrow$ no identity on $\mathbb{R}^+$

(d) has inverse for every x ? (on $\mathbb{R}^+$)

no identity $\rightarrow$ no inverse

(otherwise = solve x' for $x*x' = e$)

Chapter 3 The Definitions of Groups

(G1) $*$ is associative

(G2) $\exists$ identity $e \in G$ s.t. $x*e = e*x \ \forall x \in G$

(G3) $\exists$ inverse $x^{-1} \ \forall x \in G$ s.t. $x*x^{-1} = x^{-1}*x = e$

Exercises

A. Examples of Abelian Group

4. $x*y = \dfrac{x+y}{xy+1}$ on $\{x \in \mathbb{R} : -1 < x < 1\}$

(a) associative ?

$$x*(y*z) = x*\left(\frac{y+z}{yz+1}\right) = \frac{x+\frac{y+z}{yz+1}}{x\left(\frac{y+z}{yz+1}\right)+1} = \frac{xyz+x+y+z}{xy+xz+yz+1}$$

$$(x*y)*z = \left(\frac{x+y}{xy+1}\right)*z = \frac{\frac{x+y}{xy+1}+z}{\frac{x+y}{xy+1}z+1} = \frac{xyz+x+y+z}{xy+xz+yz+1}$$

$\Big\}$ is associative

Author: kiking

$$\frac{\frac{yz+1}{x(\frac{y+z}{yz+1})+1}}{} = \frac{xyz+x+y+z}{yz+1} \cdot \frac{yz+1}{xy+xz+yz+1} = \frac{xyz+(x+y+z)}{xy+xz+yz+1}$$

$$\frac{\left(\frac{x+y}{xy+1}\right)+z}{\left(\frac{x+y}{xy+1}\right)z+1} = \frac{x+y+z+xyz}{xy+1} \cdot \frac{xy+1}{xz+yz+xy+1} = \text{same}$$

$\Rightarrow$ is associative

is a Group

(b) $\exists$ identity ?

$$\frac{x+e}{xe+1} = x \Rightarrow x+e = x(xe+1)$$

$$x+e = ex^2+x$$

$$e(1-x^2) = 0 \rightarrow e=0$$

$e = 0$ or when $x = \pm 1$

(c) $\exists$ inverse $\forall x$?

$$x * x^{-1} = 0 \Rightarrow \frac{x+e}{xe+1} = 0$$

$$x+e = 0$$

$$e = -x$$

$$\frac{x+(-x)}{x+(-x)+1} = \frac{0}{1} = 0 \Rightarrow \exists \text{ inverse}$$

(d) Abelian Group ?

$$\frac{x+y}{xy+1} = \frac{y+x}{yx+1} \rightarrow \text{commutative} \Rightarrow \text{is Abelian Group.}$$

B Groups on the Set $\mathbb{R} \times \mathbb{R}$

2. $(a,b) * (c,d) = (ac,\ bc+d)$ on $\{(x,y) \in \mathbb{R} \times \mathbb{R} : x \neq 0\}$

y can be 0

(a) associative ?

$$(a,b) * \left((c,d) * (e,f)\right) = (a,b) * (ce,\ de+f)$$

$$= (ace,\ bce+de+f)$$

$$\left((a,b) * (c,d)\right) * (e,f) = (ac,\ bc+d) * (e,f)$$

$$= (ace,\ (bc+d)e+f)$$

$$= (ace,\ bce+de+f)$$

is associative

is a group

(b) $\exists$ identity e ?

Author: kiking

(b) ∃ identity e?

$(a,b) * (e_1, e_2) = (a,b)$

$(ae_1, be_1 + e_2) = (a,b)$

$\Rightarrow \quad ae_1 = a \Rightarrow e_1 = 1$

$be_1 + e_2 = b \Rightarrow e_2 = 0$

$\rightarrow e = (1,0)$

(c) ∃ inverse ∀x?

$(a,b) * (a^{-1}, b^{-1}) = (1,0)$

$(aa^{-1}, ba^{-1} + b^{-1}) = (1,0)$

$\Rightarrow \quad aa^{-1} = 1 \Rightarrow a^{-1} = \frac{1}{a}$

$ba^{-1} + b^{-1} = 0 \Rightarrow b^{-1} = -\frac{b}{a}$

Confirm: $(a,b) * (\frac{1}{a}, -\frac{b}{a})$

$= (1, \frac{b}{a} - \frac{b}{a}) = (1,0) \longrightarrow$ ∃ inverse

(d) is Abelian Group?

$(a,b) * (c,d) = (ac, bc+d)$

$(c,d) * (a,b) = (ca, da+b)$

$\not\rightarrow$ not commutative

→ not Abelian Group

Chapter 4 Elementary Properties of Groups

Exercises

A. Solving Equations in Groups

Let $G = \{a, b, c, x\}$. Solve x in terms of a, b and c.

3. $x^2 a = bxc^{-1}$ and $acx = xac$.

$x^2 ac = bxe$

$x(acx) = bx$

$xac = b$

$x = bc^{-1}a^{-1}$

B. Rules of Algebra in Groups

1. If $x^2 = e$ then $x = e$ Wrong
2. If $x^2 = a^2$ then $x = a$ Wrong

	I	A	B	C	D	K
I	I	A	B	C	D	K
A	A	I	C	B	K	D

Author: kiking

3. $(ab)^2 = a^2b^2$ Wrong

$(AB)^2 = C^2 = I$

$A^2B^2 = ID = D$

	I	A	B	C	D	K
I	I	A	B	C	D	K
A	A	I	C	B	K	D
B	B	K	D	A	I	C
C	C	D	K	I	A	B
D	D	C	I	K	B	A
K	K	B	A	D	C	I

4. If $x^2 = x$ then $x = e$ Correct

5. $\forall x \in G, \exists y \in G$ s.t. $x = y^2$ Wrong

e.g. $\nexists y \in G$ s.t. $C = y^2$ (diagonal checking)

6. $\forall x, y \in G, \exists z \in G$ s.t. $y = xz$ Correct (row checking)

Chapter 5 Subgroups

(SG1): closed w.r.t. multiplication (or the operation in original group)

(SG2): closed w.r.t. inverses

$F(\mathbb{R})$ = set of all functions from $\mathbb{R}$ to $\mathbb{R}$

$\langle F(\mathbb{R}), + \rangle$: a group

Subgroups:

$C(\mathbb{R})$ = all continuous functions from $\mathbb{R}$ to $\mathbb{R}$

$\mathcal{D}(\mathbb{R})$ = all differentiable functions from $\mathbb{R}$ to $\mathbb{R}$

Subgroup of G generated by a, b, and c:

the subset of G contains all the possible products of a, b, c and their inverses, e.g. abc^{-1}, $c^{-1}a^{-1}bbc$

this group is generated by $\{A, B\}$ only

	I	A	B	C	D	K
I	I	A	B	C	D	K
A	A	I	C	B	K	D
B	B	K	D	A	I	C
C	C	D	K	I	A	B
D	D	C	I	K	B	A
K	K	B	A	D	C	I

Cyclic subgroup of G, $\langle a \rangle$ with generator a

all possible products of a and a^{-1}, e.g. a, aa, aaa, ...

Author: kiking

Addition group $\mathbb{Z}_6$ is cyclic
i.e. $\mathbb{Z}_6 = \langle 1 \rangle$

$\mathbb{Z}_n$:
group of integers modulo n
operation: addition modulo n

$\mathbb{Z}_6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Defining equations completely define the multiplication table

Exercises

B Subgroup of Functions

5. $G = \langle \mathcal{D}(\mathbb{R}), + \rangle$, $H = \{ f \in \mathcal{D}(\mathbb{R}) : \frac{df}{dx} \text{ is a constant} \}$

is a subgroup
- (a) closed w.r.t. $+$?
  - $\forall f \in H$, $\frac{df}{dx}$ is constant $\to f(x) = ax + b$ for some $a, b \in \mathbb{R}$
  - $\forall f, g \in H$, $f + g = (a_1 + a_2)x + (b_1 + b_2)$ so $\frac{d(f+g)}{dx}$ is constant $\to$ closed w.r.t. $+$
- (b) closed w.r.t. inverses?
  - 0 is the identity function in $\langle \mathcal{D}(\mathbb{R}), + \rangle$
  - $-f(x) = -ax - b \to \frac{df}{dx}$ is a constant $\to$ closed w.r.t. inverses

C Subgroups of Abelian Groups

Let G : abelian group

5. Let H : subgroup of G.
   $K = \{ x \in G : x^n \in H \text{ for some } n > 0 \}$
   Prove K is a subgroup of G.

is a subgroup when G is abelian
- (a) closed w.r.t. multiplication?
  - Let $x^n \in H$, $y^m \in H \to x^n y^m \in H$ since H is a subgroup
  - $\to (x^n y^m)^k = x^{nk} y^{mk} \in H$ since $(x^n)^k \in H$, $(y^m)^k \in H$ and H abelian
  - $\to K$ is closed w.r.t. multiplication
- (b) closed w.r.t. inverses?

Author: kiking

is abelian

$\exists y' \in H$ s.t. $x^{-1}(y^2) = e$ since H is a subgroup

$\rightarrow K$ is closed w.r.t. inverses

E Generators of Groups

7. $\mathbb{Z}_2 \times \mathbb{Z}_4$ is NOT cyclic (not generated by $\langle 1,1 \rangle$)

Direct Product of Groups $= G \times H$

$= (x,y) \cdot (x',y')$

$= (xx', yy')$

$\forall x, x' \in G,\ y, y' \in H$

	(0,0)	(0,1)	(0,2)	(0,3)	(1,0)	(1,1)	(1,2)	(1,3)
(0,0)	(0,0)	(0,1)	(0,2)	(0,3)	(1,0)	(1,1)	(1,2)	(1,3)
(0,1)	(0,1)	(0,2)	(0,3)	(0,0)	(1,1)	(1,2)	(1,3)	(1,0)
(0,2)	(0,2)							
(0,3)	(0,3)							
(1,0)	(1,0)							
(1,1)	(1,1)	(1,2)	(1,3)	(1,0)	(0,1)	(0,2)	(0,3)	(0,0)
(1,2)	(1,2)							
(1,3)	(1,3)							

F Groups Determined by Generators and Defining Equations

1. Let $G = \{e, a, b, b^2, ab, ab^2\}$ whose generators satisfying $\begin{cases} a^2 = e \\ b^3 = e \\ ba = ab^2 \end{cases}$ Write the table for G.

	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab^2	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	ab^2	a	e	b
ab^2	ab^2	ab^2	a	ab	b^2	e

$a^2b = eb = b$ $\quad aba = aab^2 = a^2b^2 = b^2$

$a^2b^2 = eb^2 = b^2$ $\quad abb = ab^2$

$bab = ab^2b = ab^3 = a$ $\quad abb^2 = ab^3 = a$

$bab^2 = ab^2b^2 = ab^3b = ab$ $\quad abab = a(ab^2)b$

$b^2a = bba = bab^2 = ab^2b^2 = ab$ $\quad = a^2b^3 = e$

$b^2b^2 = eb = b$

$b^2ab = b(ab^2)b = bab^3 = ba = ab^2$ $\quad abab^2 = a(ab^2)b^2 = b$

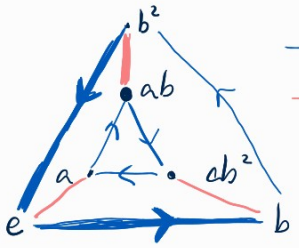
$b^2ab^2 = b(ab^2)b^2 = ab^2b = ab^3 = a$

$ab^2a = ab(ab^2)a = ab^2$ $\quad ab^2b = ab^3 = a$ $\quad ab^2b^2 = ab$

$ab^2ab = aab^2 = b^2$ $\quad ab^2ab^2 = ab(ab^2)b^2$

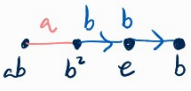
$= abab^4 = abab = e$

G Cayley Diagrams



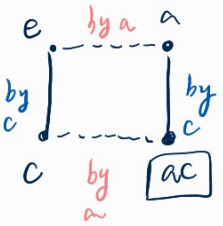
→ multiply by b

→ multiply by a — by a or a^{-1}

$(ab)(ab)^2 =$  $= b$

1. Define the group

(4 elements, 2 generators)



	e	a	ac	c
e	e	a	ac	c
a	a	e	c	ac
ac	ac	c	e	a
c	c	ac	a	e

Chapter 6 Functions

Author: kiking

Let $f: D \to T$

injective : prove if $f(a) = f(b)$, then $a = b$ $\forall a, b \in D$

surjective : prove $\forall x \in T$, $\exists y \in D$ s.t. $f(y) = x$

bijective : prove injective + surjective

Chapter 7 Groups of Permutations

Permutation of set A: a bijective function from A to A.

Symmetric Group S_A on set A

S_n: The set of all the permutations of $A = \{1, 2, \dots, n\}$.
with the operation $\circ$ of composition

S_3: $\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$\delta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\kappa = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

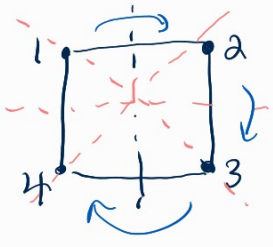
$3! = 6$ elements

$\circ$	ε	α	β	γ	δ	κ
ε	ε	α	β	γ	δ	κ
α	α	ε	γ	β	κ	δ
β	β	κ	δ	α	ε	γ
γ	γ	δ	κ	ε	α	β
δ	δ	γ	ε	κ	β	α
κ	κ	β	α	δ	γ	ε

Dihedral Group D_n:

The group of symmetries of regular polygons
with $n \geq 3$ sides

D_4: group of symmetries of the square



$R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ $R_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$

$R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ $R_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

$R_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ $R_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

$R_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ $R_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

Chapter 8 Permutations of a Finite Set

Author: kiking

(breakdown) (breakdown)

Permutations → Cycles → Transpositions (cycle of length 2)

e.g. in S_6, cycle (1426) cycle (254)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 2 & 5 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 2 & 4 & 6 \end{pmatrix}$$

cycle of length 4 cycle of length 3

product of cycles $(245)(124)$ in S_5

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$$

Even permutations : permutation with even num of transpositions

Odd permutations : ——— odd ———

A_n : the Alternating group on the set $\{1, 2, \dots, n\}$

= The set of all even permutations in S_n

(is a subgroup of S_n ;

& the identity permutation is even)

Chapter 9 Isomorphism

Isomorphism between groups G_1 and G_2 :

A bijective function $f: G_1 \to G_2$ satisfying

$\forall a, b \in G_1$, $f(ab) = f(a) f(b)$

e.g. $\langle \mathbb{R}, + \rangle \overset{\text{isomorphic}}{\cong} \langle \mathbb{R}^{pos}, \cdot \rangle$ with function $f(x) = e^x$

is isomorphic

(i) f is injective : if $e^a = e^b$ then $a = b$

(ii) f is surjective : $\forall x \in \mathbb{R}^{pos}$, $\exists y = \ln(x) \in \mathbb{R}$ s.t. $f(\ln x) = x$

(iii) $f(a+b) = e^{a+b} = e^a \cdot e^b = f(a) \cdot f(b)$

Cayley's Theorem : (Arthur Cayley)

every group is isomorphic to a group of permutations

Proof : Let G be a group

Author: kiking

Let $G^* = \{ \pi_a : a \in G \}$ where $\pi_a : G \to G$ is defined as

Left Representation of group G $\longrightarrow$ $\pi_a(x) = ax. \quad \forall x \in G$

if G commutative: left representation = right representation

✡ π_a is a permutation $\forall a \in G$.

(i) π_a is injective: if $ax_1 = ax_2$, then $x_1 = x_2$

(ii) π_a is surjective: $\forall x \in G$, $\exists y = a^{-1}x \in G$ s.t. $\pi_a(y) = \pi_a(a^{-1}x) = a(a^{-1}x) = x$

π_a is bijective mapping $G \to G \Rightarrow$ a permutation

✡ G^* is a subgroup of S_G (the group of all permutations)

(i) closed w.r.t. compositions:

$\pi_a \circ \pi_b = abx = \pi_{ab} \in G^*$

(ii) closed w.r.t. inverses:

π_e is the identity permutation: $\pi_e(x) = ex = x$

a^{-1} exists so $\pi_{a^{-1}}$ is the inverse of π_a: $\pi_{a^{-1}}(x)\,\pi_a(x) = x$

$\to G^*$ is a subgroup of S_G

✡ Now G is isomorphic to G^* (the selected subgroup of permutations of G)

Let $f : G \to G^*$ be defined as $f(a) = \pi_a$

(i) f is injective: $\pi_a = \pi_b \Rightarrow a = b$

(ii) f is surjective: $\forall \pi_a \; \exists \, a \in G$

(iii) $f(ab) = \pi_{ab} = abx = a(bx) = \pi_a \circ \pi_b = f(a) \cdot f(b)$

$\to f$ is an isomorphism, so $G \cong G^*$

Exercises

C. Isomorphism of Some Finite Groups

4. S_3:

$\circ$	ε	α	β	γ	δ	κ
ε	ε	α	β	γ	δ	κ
α	α	ε	γ	β	κ	δ
β	β	κ	δ	α	ε	γ
γ	γ	δ	κ	ε	α	β
δ	δ	γ	ε	κ	β	α
κ	κ	β	α	δ	γ	ε

Another:

	I	A	B	C	D	K
I	I	A	B	C	D	K
A	A	I	C	B	K	D
B	B	K	D	A	I	C
C	C	D	K	I	A	B
D	D	C	I	K	B	A
K	K	B	A	D	C	I

Isomorphic by $f = \begin{pmatrix} \varepsilon & \alpha & \beta & \gamma & \delta & \kappa \\ I & A & B & C & D & K \end{pmatrix}$

I. Group Automorphisms

Author: kiking

Automorphism = an isomorphism from G to G.

1. In $\mathbb{Z}_6$,

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} : \mathbb{Z}_6 \to \mathbb{Z}_6$$

(i) f is injective
(ii) f is surjective
(iii) $f(xy) = f((x+y) \bmod 6)$ $\quad x=2, y=5$

$= $ remainder of $(x+y) \bmod 6$ $\quad 5$

$f(x)f(y) = ($remainder of $x \bmod 6$ + remainder of $y \bmod 6) \bmod 6$
$\quad 4 \qquad\qquad 1$

$= f(xy)$

$\hookrightarrow$ Isomorphism $\to$ automorphism

Chapter 10 Order of Group Elements

Order of the element a : the least positive integer n s.t. $a^n = e$ or if no such integers, the order is infinity.

Exercises E. Let $a, b \in G$, $\text{ord}(a)=m$, $\text{ord}(b)=n$.
If m, n relatively prime, then $a^i b^j$ $\begin{pmatrix} 0 \le i < m \\ 0 \le j < n \end{pmatrix}$ are all distinct.

Chapter 11 Cyclic Groups

Suppose $\langle a \rangle$ is a cyclic group whose generator has order n.

$\langle a \rangle = \{a^0, a^1, a^2, \dots, a^{n-1}\}$ $\quad \text{ord}(a) = n \Rightarrow |\langle a \rangle| = n$ (order of generator; order of group)

$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ (group of integers modulo n)

$f(i) = a^i$ is an isomorphism from $\mathbb{Z}_n \to \langle a \rangle$

so $\mathbb{Z}_n \cong \langle a \rangle$

Every cyclic group of order n is isomorphic to $\mathbb{Z}_n$
Every cyclic group of order infinity is isomorphic to $\mathbb{Z}$
Every subgroup of a cyclic group is cyclic

Chapter 12 Partitions and Equivalence Relations

$\sim$: the equivalent relation determined by the partition $\{A_i : i \in I\}$

Author: kiking

(i) Reflexive : $x \sim x \quad \forall x$ in A

(ii) Symmetric : if $x \sim y$, then $y \sim x$

(iii) Transitive : if $x \sim y$ and $y \sim z$, then $x \sim z$

Equivalent class $[x] = \{y \in A : y \sim x\}$

If $x \sim y$, then $[x] = [y]$

The family of all equivalent classes $\{[x] : x \in A\}$ is a partition of A

each partition of A determines / is determined by one equivalent relation on A.

Partition : a family $\{A_i : i \in I\}$ of nonempty subsets of A s.t.

(P1) if $x \in A_i$ and $x \in A_j$, then $A_i = A_j$

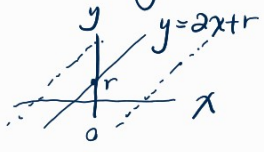
(P2) $\forall x \in A$, $x \in A_i$ for some $i \in I$

Exercises

C. Equivalence Relations and Partitions of $\mathbb{R} \times \mathbb{R}$

1. $\forall r \in \mathbb{R}$, $A_r = \{(x,y) : y = 2x + r\}$.

Geometrically each partition is a line with slope 2 and intercept r



$(x,y) \sim (u,v)$ if they lie on the same slope

(i) Suppose $(u,v) \in A_r$ and $(u,v) \in A_s$

then $v = 2u + r = 2u + s \Rightarrow r = s$

Hence $A_r = A_s$

(ii) $\forall x, y \in \mathbb{R}$, $y = 2x + r \Rightarrow r = y - 2x \in \mathbb{R}$

Hence (x,y) always lie in the class A_{y-2x}

D. Equivalent Relations on Groups

5. $a \sim b$ iff ab^{-1} commutes with every $x \in G$

(i) reflexive

$aa^{-1} \cdot x = x \cdot aa^{-1} \quad \forall x \Rightarrow a \sim a$

(ii) symmetric

Since $a \sim b$, $ab^{-1}x = xab^{-1}$

$ab^{-1}xb = xa$

$ab^{-1}xba^{-1} = x$

$b^{-1}xba^{-1} = a^{-1}x$

Author: kiking

$xba^{-1} = ba^{-1}x \longrightarrow b \sim a$

(iii) transitive

$a \sim b$ and $b \sim c$,

$ab^{-1}(xbc^{-1})x = x(ab^{-1})bc^{-1}$

$xab^{-1}bc^{-1}x = x\,xab^{-1}bc^{-1}$

$xac^{-1}x = x\,xac^{-1}$

$ac^{-1}x = xac^{-1} \longrightarrow a \sim c$

$ab^{-1}x = xab^{-1}$ and $bc^{-1}x = xbc^{-1}$

$\Downarrow$?

$ac^{-1}x = xac^{-1}$

→ is an equivalent relation

Equivalent class $[x] = \{y \in G : yx^{-1}z = zyx^{-1}\ \forall z \in G\}$

Chapter 13 Counting Cosets

Let G be a group, H be a subgroup.

left coset aH Ha right coset

denotes the set of all products ha, as a fixed, h ranges over H

If $a \in Hb$, then $Ha = Hb$

since $a = h_1 b$ for some $h_1 \in H$,

$\forall x \in Ha$, $x = h_2 a = (h_2 h_1)b \in Hb$

① Thm $\{Ha : a \in G\}$ is a partition of G

(i) suppose $x \in Ha$ and $x \in Hb$

then $x = h_1 a = h_2 b$ for some $h_1, h_2 \in H$

$\Rightarrow a = (h_1)^{-1} h_2 b$ and $(h_1)^{-1} h_2 \in H$

$\Rightarrow a \in Hb \Rightarrow Ha = Hb$

(ii) Any $x \in G = x \in H_x$ because $x = ex$

→ is a partition

② Thm H and Ha has a one-one correspondence, for any coset Ha

Define $f : H \to Ha = f(h) = ha$

(i) injective : $f(h_1) = f(h_2) \Rightarrow h_1 = h_2$

(ii) surjective : $\forall x = h_x a \in Ha$, $f(h_x) = x$

→ one-one correspondence

Author: kiking

(3) Lagrange's Theorem

Let G be finite group, H any subgroup.

Then $|G|$ is a multiple of $|H|$ (the order of G = multiple of order of H)

> Proof: since any coset Ha has the same order (# elements) as H, and the family of cosets $\{Ha\}$ is a partition of G.

(4) Thm

If a group G has prime number of elements, then G is a cyclic group; any element $\neq e$ is a generator

> Proof: the subgroup is unique (up to isomorphism) since it must has a prime order equal to the order of G by Lagrange Theorem. E.g. $\mathbb{Z}_7$, $\mathbb{Z}_{11}$

Index of H in G $\quad G:H$ – the number of cosets of H in G

Exercises

B. Examples of Cosets in Infinite Groups

1. The subgroup $\langle 3 \rangle$ in $\mathbb{Z}$ (with + as operator)

$\langle 3 \rangle = \{ -3^3, -3^2, -3^1, 1, 3, 3^2, 3^3, \dots \}$

Cosets $= \{ \langle 3 \rangle + 1, \langle 3 \rangle + 2, \langle 3 \rangle + 0 \}$

E Elementary Properties of Cosets

Cauchy's Theorem

if G is a finite group, and p is a prime divisor of $|G|$, then G has an element of order p.

Survey of all possible groups whose order is ≤ 10

Prime-related:

Group with 2, 3, 5, 7 elements: $G \approx \mathbb{Z}_p$ (the unique cyclic group)

Group with 4, 9 elements: $G \approx \mathbb{Z}_{p^2}$ or $G \approx \mathbb{Z}_p \times \mathbb{Z}_p$

Author: kiking

Groups with 6 elements

the group must have elements with order 2 and order 3. (Cauchy)

$\Rightarrow \{e, a, b, b^2, ab, ab^2\}$ must be distinct by Chapter 10 Exercise E.

$\Rightarrow$ if $ba = ab$, then $G \cong \mathbb{Z}_6$

if $ba = ab^2$, then $G \cong S_3$

$\mathbb{Z}_6$ and S_3 are the only possible groups (up to isomorphism)

Groups with 10 elements

the group must have elements with order 2 and 5 (Cauchy)

$\Rightarrow \{e, a, b, b^2, b^3, b^4, ab, ab^2, ab^3, ab^4\}$ must be distinct

$\Rightarrow$ if $ba = ab$, then $G \cong \mathbb{Z}_{10}$

$ba \neq ab^2$, $ba \neq ab^3$

if $ba = ab^4$, then $G \cong D_5$

$\mathbb{Z}_{10}$ and D_5 are the only possible groups (up to isomorphism)

Group with 8 elements

If G has an element of order 8 $\Rightarrow G \cong \mathbb{Z}_8$

Assume $n_0 =$

if every $x \neq e$ in G has order 2

$\Rightarrow \{e, a, b, c, ab, ac, bc, abc\}$ are distinct $\Rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

if G has an element of order 4

$\Rightarrow$ Let $H = \{e, a, a^2, a^3\}$, Let $b \in G$ but $b \notin H$ and $H_b = \{b, ab, a^2b, a^3b\}$.

By Lagrange's Theorem, $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$

$\Rightarrow$ Assume there is an element in H_b that has order 2

$\Rightarrow$ if $ba = ab \Rightarrow G \cong \mathbb{Z}_4 \times \mathbb{Z}_4$ $\quad ba \neq a^2b$

if $ba = a^3b \Rightarrow G \cong D_4$

$\Rightarrow$ Assume not, $\{b, ab, a^2b, a^3b\}$ all have order 4

$\Rightarrow a^4 = b^4 = e$, $a^2 = b^2$, $ba = a^3b$ completely determines G

Quarterion group $Q \Rightarrow \mathbb{Z} \cong Q$

$\therefore$ The only groups (up to isomorphism) are $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, D_4, and Q.

I Conjugate Elements

Conjugate of a : $\{x \in G : xax^{-1}\}$

Author: kiking

1. "a is equal to a conjugate of b" is an equivalence relation

(a) Reflexive
if $a = eae^{-1} \Rightarrow$ a is equal to a conjugate of a

(b) Symmetric
if $a = xbx^{-1} \Rightarrow b = x^{-1}ax = (x^{-1})a(x^{-1})^{-1}$
$\Rightarrow$ b is equal to a conjugate of a

(c) Transitive
$a = xbx^{-1}$, $b = xcx^{-1}$
$a = x(xcx^{-1})x^{-1} = (x)^2 c (x^{-1})^2 \Rightarrow$ a is equal to a conjugate of c

$\Rightarrow$ is a equivalence relation

Centralizer of a: $C_a = \{x \in G : xa = ax\}$ elements commutes with a
$= \{x \in G : xax^{-1} = a\}$

5. There is a one-one correspondence between
the sets of all Conjugates of a
and the sets of all cosets of Centralizers of a

6. The size of every conjugate class is a factor of $|G|$

J. Group Acting on a Set

Let A be a set.
G be any subgroups of S_A
$\Rightarrow$ a subgroup of permutations of A $\Rightarrow$ a group Acting on a set A

Orbit of $u \in A$: $O(u) = \{g(u) : g \in G\}$

define $u \sim v$ iff $g(u) = v$; $\sim$ is equivalent relation
and orbits are equivalent classes

Stabalizer of $u \in A$: $G_u = \{g \in G : g(u) = u\}$
the set of all permutations in G which leave u fixed.

3. Let $\alpha = (12)(34)(56)$
$\beta = (23)$ in S_6.

Let $G = \{\varepsilon, \alpha, \beta, \alpha\beta, \beta\alpha, \alpha\beta\alpha, \beta\alpha\beta, (\alpha\beta)^2\}$ be a subgroup of S_6

$O(1) = \{g(1) : g \in G\} = \{1, 2, 1, 2, 3, 4, 3, 4\} = \{1, 2, 3, 4\}$
$O(2) = \{g(2) : g \in G\} = \{2, 1, 3, 4, 1, 2, 4, 3\} = \{1, 2, 3, 4\}$
$G(1) = \{g \in G : g(1) = 1\} = \{\varepsilon, \beta\}$
$G(2) = \{g \in G : g(2) = 2\} = \{\varepsilon, \alpha\beta\alpha\}$

$\alpha(2) = 1$
$\beta(1) = 1$
$\alpha(1) = 2$

Author: kiking

Chapter 14 Homomorphisms

Let G, H be groups.

Homomorphism from G to H:

A function $f: G \to H$ s.t. $\forall a, b \in G$,

$$f(a,b) = f(a)\,f(b)$$

$\Rightarrow H$ is a homomorphic image of G.

Example:

$\mathbb{Z}_6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

homomorphic image

$\mathbb{Z}_3$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\mathbb{Z} \to P =$

+	e	o
e	e	o
o	o	e

where f carries all even integers to e, odd integers to o

$$f(r+s) = f(r) + f(s)$$

① **Thm** G, H groups, $f: G \to H$ a homomorphism. Then

(i) $f(e) = e$

(ii) $f(a^{-1}) = [f(a)]^{-1}$ $\forall a \in G$.

Normal subgroup H of G:

closed w.r.t. multiplication, inverses

If H is a subgroup of G and

H is closed w.r.t. conjugates, i.e.

$$xax^{-1} \in H \quad \forall a \in H, \forall x \in G$$

Kernel of the homomorphism $f: G \to H$:

$$\ker(f) = K = \{ x \in G : f(x) = e_H \}$$

all elements of G carried by f onto the identity element of H.

② **Thm** Let $f: G \to H$ be a homomorphism.

(i) $\ker(f)$ is a Normal subgroup of G

Author: kiking

(a) closed w.r.t. multiplications ?
$a, b \in \ker(f) \Rightarrow f(a) = e \quad f(b) = e$
$f(ab) = f(a) f(b)$ (homomorphism)
$= e$
$\therefore ab \in \ker(f)$

(b) closed w.r.t. inverses ?
$f(a^{-1}) = [f(a)]^{-1}$ (homomorphism)
$= e^{-1}$
$= e$
$\therefore a^{-1} \in \ker(f)$

is a subgroup

(c) closed w.r.t. conjugates?
$f(xax^{-1}) = f(x) f(a) f(x^{-1})$ (homomorphism)
$= f(x) e f(x^{-1})$
$= f(x)[f(x)]^{-1}$ (homomorphism)
$= e$
$\therefore xax^{-1} \in \ker(f)$ for any $x \in G$

is a Normal subgroup

(ii) range of f is a subgroup of G

Exercises

G. Properties preserved under Homomorphism

Let $f: G \to H$ be a homomorphism. Then
- If G is abelian, then H is abelian
- If G is a cyclic group, then H —"—
- If every element of G has finite order, then H —"—
- If every element of G has its own inverse, then H —"—
- If every element of G has a square root, then H —"—
- If G is finitely generated (finite number of generators), then H —"—

D. Basic Properties of Normal Subgroups

3. Every subgroup of an abelian group is normal.

Let G be a abelian group, H be a subgroup of G.
Let $x \in G$, $a \in H$.
$xax^{-1} = (xx^{-1})a$ (abelian)
$= a \in H$.
Hence H is normal

Chapter 15 Quotient Groups

Thm If H is a normal subgroup of G,

Author: kiking

then $aH = Ha$ for every $a \in G$.

Proof: Let $x \in aH$.
$x = ah_1$ for some $h_1 \in H$.
and $ah_1a^{-1} \in H$ since H is closed w.r.t. conjugate.
Then $x = ah_1(a^{-1}a)$
$= (ah_1a^{-1})a \in Ha$ $\therefore aH = Ha \ \forall a \in G$

Thm Let H be a normal subgroup of G.
If $Ha = Hc$ and $Hb = Hd$,
then $H(ab) = H(cd)$ where $H(ab) = Ha \cdot Hb$
$H(cd) = Hc \cdot Hd$

Proof: Since $a \in Hc$, $b \in Hd$,
$ab = h_1c \cdot h_2d$
$= h_1(ch_2)d$
$= h_1(h_3c)d$ ← since $ch_2 \in cH = Hc$ when H is normal
$= (h_1h_3)cd \in H(cd)$

Quotient Group of G by H

Let G a group, H a normal subgroup
$G/H = \{Ha, Hb, Hc, \dots\}$ = all cosets of H
with coset multiplication $Ha \circ Hb = H(a,b)$ is a Group

Proof of G/H is a group:
(i) associative
$Ha(bc) = Ha \cdot (Hb \circ Hc)$
$= h_1a \cdot h_2b \cdot h_3c$
$= (Ha \cdot Hb) \cdot Hc = H(ab)c$
(ii) $\exists$ identity
He is the identity since $Hae = Ha \cdot He = He \cdot Ha$
$= Ha$
(iii) $\exists$ inverse
$\forall Ha$, $Ha^{-1} \circ Ha = He$

Thm G/H is a homomorphic image of G.
Consider $f: G \to G/H$ where $f(x) = Hx$ Natural homomorphism
$f(xy) = Hxy = Hx \circ Hy = f(x)f(y)$ so f is a homomorphism

Quotient group construction = Manufacturing all homomorphic images

Quotient group ... Homomorphic images

Example

In $\langle \mathbb{Z}, + \rangle$, $\langle 6 \rangle$ is a Normal subgroup (since $\mathbb{Z}$ is abelian).

Consider the Quotient group $\mathbb{Z}/\langle 6 \rangle$:

cosets of the subgroup $\langle 6 \rangle$: $\{\langle 6 \rangle + 0 \ \langle 6 \rangle + 1 \ \dots \ \langle 6 \rangle + 5\}$

Then $\mathbb{Z}/\langle 6 \rangle$ consists of 6 elements, write as $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$:

and can be seen as $\mathbb{Z}_6$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

For any n, $\mathbb{Z}_n$ is a homomorphic image of $\mathbb{Z}$

⑤ Thm G be a group, H be a subgroup.

(i) $Ha = Hb$ iff $ab^{-1} \in H$ for $a = h_1 b \Rightarrow ab^{-1} = h \in H$

(ii) $Ha = H$ iff $a \in H$

Choose H so as to "factor out" unwanted properties of G, and preserve in G/H only "desirable" traits.

Examples

Let G be an abelian group,

H consists of all elements having finite order.

Quotient group G/H : no element except identity have finite order.

suppose $Hx \in G/H$ has finite order.

then $\exists\, m \neq 0$ s.t. $(Hx)^m = H$ (the neutral element)

$Hx^m = H$

$x^m \in H$ (by ⑤ (ii))

so $(x^m)^k = e \Rightarrow x \in H \Rightarrow Hx = H$ (by ⑤ (ii))

∴ the only element having finite order is H the neutral element

Commutator : $\{a, b \in G : aba^{-1}b^{-1}\}$ $aba^{-1}b^{-1} = e$ iff $ab = ba$

the number of distinct commutators in a group G

is a measure of the extent to which G departs from commutative

Let H: subgroup which contains all the commutators of G,

then G/H is abelian : no element except identity is a commutator

$Hyx = Hxy$ iff $yx(xy)^{-1} \in H$

$\Leftrightarrow$ $yxy^{-1}x^{-1} \in H$ satisfied since H contains all commutators

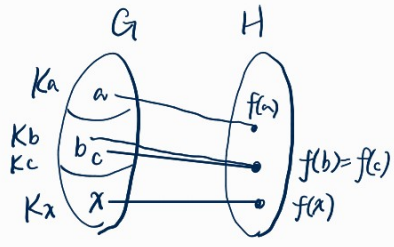
Author: kiking

Chapter 16 The Fundamental Homomorphism Theorem

Every homomorphic image of G is isomorphic to a quotient group of G. by the kernel of f

① **Thm** Let $f: G \to H$ be a homomorphism with kernel K.
Then $f(a) = f(b)$ iff $Ka = Kb$

Proof: $f(a) = f(b) \Leftrightarrow f(a)[f(b)]^{-1} = e$
$\Leftrightarrow f(ab^{-1}) = e$ (by homomorphism)
$\Leftrightarrow ab^{-1} \in K$
$\Leftrightarrow Ka = Kb$ (by Thm ⑤(ii))



② **Thm** The Fundamental Homomorphism Theorem
Let $f: G \to H$ be a homomorphism of G onto H.
If K is the kernel of f, then

$$H \cong G/K$$

If $f: G \xrightarrow[K]{} \!\!\!\rightarrow H$ then $H \cong G/K$

Proof: Define $\phi: G/K \to H$ as
$\phi(Kx) = f(x)$

(a) ϕ uniquely defined?
by Thm ① if $Ka = Kb$, then $f(a) = f(b)$

(b) ϕ injective?
if $\phi(Ka) = \phi(Kb)$, $f(a) = f(b) \Rightarrow a = b$ since f injective

(b) ϕ surjective?
$\forall f(x) \in H$, $\exists Kx$ s.t. $\phi(Kx) = f(x) \Rightarrow$ surjective

(c) $\phi(KaKb) = f(ab) = f(a)f(b) = \phi(Ka)\phi(Kb)$ (f homomorphism)

→ ϕ is an isomorphism

Example

$f = \begin{pmatrix} a & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$ from $\mathbb{Z}_6 \to \mathbb{Z}_3$.

$\ker(f) = \{0, 3\} = \langle 3 \rangle$. By FHT,

Author: kiking

$f: \mathbb{Z}_6 \xrightarrow{(3)} \mathbb{Z}_3 \Rightarrow \mathbb{Z}_3 \cong \mathbb{Z}_6/\langle 3 \rangle$

Exercises

B. Example of the FHT applied to $\mathcal{F}(\mathbb{R})$.

Let $\alpha: \mathcal{F}(\mathbb{R}) \to \mathbb{R}$ be defined by $\alpha(f) = f(1)$

$\beta: \mathcal{F}(\mathbb{R}) \to \mathbb{R}$ be defined by $\beta(f) = f(0)$.

1. α, β are homomorphisms from $\mathcal{F}(\mathbb{R})$ to $\mathbb{R}$

   $\alpha(f_1 f_2) = f_1 f_2(1) = \alpha(f_1)\alpha(f_2)$. .....

2. Let J : the set of all functions whose graph passes through $(1,0)$

   K : ——— " ——— $(2,0)$.

   $\forall f \in J,\ \alpha(f) = f(1) = 0 \Rightarrow J$ is a kernel of α ....

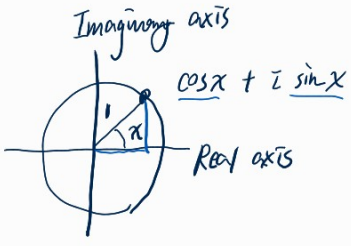
   By F.H.T, $\mathbb{R} \cong \mathcal{F}(\mathbb{R})/J$ and $\mathbb{R} \cong \mathcal{F}(\mathbb{R})/K$

3. Hence, $\mathcal{F}(\mathbb{R})/J \cong \mathcal{F}(\mathbb{R})/K$ for any J, K whose graphs pass throughs $(x,0)$ for some x

H. Quotient Groups Isomorphic to the Circle Group

The unit circle consisting of all the complex numbers can be written in the form

$$\operatorname{cis} x = \cos x + i \sin x$$



(1) & (2) : $\langle T, \circ \rangle$ is a circle group

where $T = \{\operatorname{cis} x : x \in \mathbb{R}\}$

and $\circ : \operatorname{cis}(x+y) = \operatorname{cis}(x)\operatorname{cis}(y)$

(3)–(5) : Let $f(x) = \operatorname{cis} x$. $f: \mathbb{R} \xrightarrow[\langle 2\pi \rangle = \{2n\pi : n \in \mathbb{Z}\}]{\text{kernel}} T$

By FHT,

$$\mathbb{R}/\langle 2\pi \rangle \cong T.$$

(6)–(7) : Let $g(x) = \operatorname{cis} 2\pi x$. $g: \mathbb{R} \xrightarrow[\mathbb{Z}]{\text{kernel}} T$

By FHT,

$$\mathbb{R}/\mathbb{Z} \cong T.$$

I. First Isomorphism Theorem

Let G be a group; H, K subgroups, and H a normal subgroup.

The function $f(k) = Hk$ is a homomorphism $f: K \xrightarrow[(H \cap K)]{} HK/H$

By FHT, $K/(H \cap K) \cong HK/H$

J. Second Isomorphism Theorem

Let H, K be normal subgroups and $H \subseteq K$.

The function $\phi(Ha) = Ka$ is a homomorphism

Author: kiking

$\phi : G/H \xrightarrow{K/H} G/K$

By FHT, $(G/H) / (K/H) \cong G/K$

M. p-Sylow Subgroups

p-group = a finite group G with every element x in G has a power p where p is prime.

p-subgroup = when H is a p-group and H is a subgroup of G.

p-Sylow subgroup = when K is a p-subgroup and K is maximal (K not contained in other larger p-subgroup)

N. Sylow's Theorem

Let G be a finite group and p a prime number.
$\forall n$ s.t. p^n divides $|G|$, G has a subgroup of order p^n.

P. Decomposition of a Finite Abelian Group into p-Groups

Suppose $|G| = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ (prime factorization)

Then $G \cong G_1 \times G_2 \times \cdots \times G_n$ where G_i is a p_i-group.

Q. Basis Theorem for Finite Abelian Groups

Every finite abelian group is a direct product of cyclic groups of prime power order.

Chapter 17 Rings : definitions and elementary properties

Examine algebraic systems with two operations instead of just one.

Ring : a set A with operations $+$, $\times$ (multiplication) satisfying :

(R1) : $\langle A, + \rangle$ is a Abelian group

(R2) : $\times$ (multiplication) is associative

(R3) : $\times$ (multiplication) is distributive over $+$

i.e. $\forall a, b, c \in A$, $a(b+c) = ab + ac$
$(b+c)a = ba + ca$

Thm Let $a, b \in$ ring A.

(i). $a \cdot 0 = 0 \cdot a = 0$] define multiplication

Author: kiking

(ii) $a(-b) = (-a)b = -(ab)$
(iii) $(-a)(-b) = ab$

with the additive-neutral element (0) and with additive-inverses (negatives)

Examples:

the ring of the integers $\mathbb{Z}$ with $+, \times$
rational numbers $\mathbb{Q}$
real numbers $\mathbb{R}$
complex numbers $\mathbb{C}$
the ring of the real functions $\mathcal{F}(\mathbb{R})$
where $[f+g](x) = f(g)+f(x)$
$[fg](x) = f(x)\,g(x)$ $\forall x \in \mathbb{R}$

} Infinite rings

$\mathbb{Z}_n$ with addition modulo n
multiplication modulo n
is a finite ring

"Optional features" of Ring:

① a Commutative Ring: when multiplication is also commutative

② a Ring with Unity: when $\exists$ a neutral element for multiplication, denoted by 1.

③ with invertible elements: elements with multiplicative inverses

Field = ① + ② + ③ = a commutative ring with unity in which every non-zero element is invertible

Examples: infinite fields: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
finite fields: $\mathbb{Z}_5$

④ with cancellation property: iff no divisors of zero
i.e. nonzero b s.t. $ab=0$ when $a \neq 0$

if $ab=ac$ / $ba=ca$
implies $b=c$
$\forall\, a \neq 0, b, c \in$ ring A

Integral Domain = ① + ② + ④ = a commutative ring with unity having the cancellation property e.g. $\mathbb{Z}$

Fields are Integral Domains;

Author: kiking

but Integral Domains might not be Fields, e.g. $\mathbb{Z}$