

# Title

D. Zack Garza

August 17, 2019

## Contents

<b>1</b>	<b>List of Topics</b>	<b>2</b>
<b>2</b>	<b>Groups</b>	<b>4</b>
2.1	Definitions . . . . .	4
2.1.1	<b>Subgroup Generated</b> by a set $A$ . . . . .	4
2.1.2	<b>Free Group</b> on a set $X$ . . . . .	4
2.1.3	<b>Centralizer</b> of an element or a subgroup . . . . .	4
2.1.4	<b>Center</b> of a group . . . . .	4
2.1.5	<b>Normalizer</b> of a subgroup . . . . .	4
2.1.6	<b>Normal Core</b> of a subgroup . . . . .	5
2.1.7	<b>Normal Closure</b> of a subgroup . . . . .	5
2.1.8	<b>Group Action</b> of a group on a set . . . . .	5
2.1.9	<b>Transitive</b> group actions . . . . .	6
2.1.10	<b>Orbit</b> of a set element . . . . .	6
2.1.11	<b>Stabilizer</b> of a set element . . . . .	6
2.1.12	<b>Automorphisms</b> of a group . . . . .	6
2.1.13	<b>Inner Automorphisms</b> of a group . . . . .	7
2.1.14	<b>Outer Automorphisms</b> of a group . . . . .	7
2.1.15	<b>Conjugacy Class</b> of an element . . . . .	7
2.1.16	<b>Characteristic</b> subgroup . . . . .	7
2.1.17	<b>Simple</b> group . . . . .	7
2.1.18	<b>Commutator</b> of an element, or of subgroups . . . . .	7
2.2	Structural Results . . . . .	7
2.2.1	Isomorphisms Theorems . . . . .	8
2.3	Misc Results . . . . .	8
2.4	Numeric Results . . . . .	9
2.4.1	Cauchy's Theorem . . . . .	9
2.4.2	Sylow Theorems: $ G  = p^k m$ where $p \nmid m$ . . . . .	9
2.4.3	Orbit-stabilizer Theorem . . . . .	9
2.4.4	Burnside's Lemma . . . . .	10
2.4.5	The class equation . . . . .	10
2.4.6	General facts . . . . .	10
2.5	Common Groups . . . . .	11
2.5.1	$S_3$ . . . . .	11

2.5.2	$S_n$	11
2.5.3	$A_n$	11
2.5.4	$D_n$	11
<b>3</b>	<b>Rings</b>	<b>12</b>
3.1	Facts about ideals:	12
3.2	Maximal ideals	12
3.3	Prime ideals	12
3.4	Radicals	12

# 1 List of Topics

Chapters 1-9 of Dummit and Foote

- Left and right cosets
- Lagrange's theorem
- Isomorphism theorems
- Group generated by a subset
- Structure of cyclic groups
- Composite groups
  - $HK$  is a subgroup iff  $HK = KH$
- Normalizer
  - $HK \leq H$  if  $H \leq N_G(K)$
- Symmetric groups
  - Conjugacy classes are determined by cycle types
- Group actions
  - Actions of  $G$  on  $X$  are equivalent to homomorphisms from  $G$  into  $\text{Sym}(X)$
- Cayley's theorem
- Orbits of an action
- Orbit stabilizer theorem
- Orbits act on left cosets of subgroups
- Subgroups of index  $p$ , the smallest prime dividing  $|G|$ , are normal
- Action of  $G$  on itself by conjugation
- Class equation
- $p$ -groups
  - Have non trivial center
- $p^2$  groups are abelian
- Automorphisms, the automorphism group
  - Inner automorphisms
  - $\text{Inn}(G) \cong Z/Z(G)$
  - $\text{Aut}(S_n) = \text{Inn}(S_n)$  unless  $n = 6$
  - $\text{Aut}(G)$  for cyclic groups
  - $G \cong Z_p^n$ , then  $\text{Aut}(G) \cong GL_n(Z_p)$
- Proof of Sylow theorems
- $A_n$  is simple for  $n \geq 5$
- Recognition of internal direct product
- Recognition of semi-direct product

- Classifications:
  - $pq$
- Free group & presentations
- Commutator subgroup
- Solvable groups
  - $S_n$  is solvable for  $n \leq 4$
- Derived series
  - Solvable iff derived series reaches  $e$
- Nilpotent groups
  - Nilpotent iff all sylow-p subgroups are normal
  - Nilpotent iff all maximal subgroups are normal
- Upper central series
  - Nilpotent iff series reaches  $G$
- Lower central series
  - Nilpotent iff series reaches  $e$
- Fratini's argument
- Rings
  - $I$  maximal iff  $R/I$  is a field
  - Zorn's lemma
  - Chinese remainder theorem
  - Localization of a domain
  - Field of fractions
  - Factorization in domains
  - Euclidean algorithm
  - Gaussian integers
  - Primes and irreducibles
  - Domains
    - \* Primes are irreducible
  - UFDs
    - \* Have GCDs
    - \* Sometimes PIDs
  - PIDs
    - \* Noetherian
    - \* Irreducibles are prime
    - \* Are UFDs
    - \* Have GCDs
  - Euclidean domains
    - \* Are PIDs
  - Factorization in  $Z[i]$
  - Polynomial rings
  - Gauss' lemma
  - Remainder and factor theorem
  - Polynomials
  - Reducibility
  - Rational root test
  - Eisenstein's criterion

## 2 Groups

### 2.1 Definitions

#### 2.1.1 Subgroup Generated by a set $A$

- $\langle A \rangle = \{a_1^{\pm 1}, a_2^{\pm 1}, \dots, a_n^{\pm 1} : a_i \in A, n \in \mathbb{N}\}$
- Equivalently, the intersection of all  $H$  such that  $A \subseteq H \leq G$

#### 2.1.2 Free Group on a set $X$

- Equivalently, words over the alphabet  $X$  made into a group via concatenation

#### 2.1.3 Centralizer of an element or a subgroup

- $C_G(a) = \{g \in G : ga = ag\}$

•

$$C_G(H) = \{g \in G : \forall h \in H, gh = hg\} = \bigcap_{h \in H} C_G(h)$$

– Note - requires the same  $g$  on both sides!

- Facts:

- $C_G(H) \leq G$
- $C_G(H) \trianglelefteq N_G(H)$
- $C_G(G) = Z(G)$
- $C_H(a) = H \cap C_G(a)$

#### 2.1.4 Center of a group

- $Z(G) = \{g \in G : \forall x \in G, gx = xg\}$

- Facts

–

$$Z(G) = \bigcap_{a \in G} C_G(a)$$

#### 2.1.5 Normalizer of a subgroup

•

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

- Equivalently,  $\bigcup \{K : H \trianglelefteq K \leq G\}$  (the largest  $K \leq G$  for which  $H \trianglelefteq K$ )
- Equivalently, the stabilizer of  $H$  under  $G$  acting on its subgroups via conjugation
- Differs from centralizer; can have  $gh = h'g$
- Facts:
  - $C_G(H) \leq N_G(H) \leq G$
  - $N_G(H)/C_G(H) \cong A \leq \text{Aut}(H)$

- Given  $H \subseteq G$ , let

$$S(H) = \bigcup_{g \in G} gHg^{-1}$$

, so  $|S(H)|$  is the number of conjugates to  $H$ . Then

$$|S(H)| = [G : N_G(H)]$$

\* i.e. the number of subgroups conjugate to  $H$  equals the index of the normalizer of  $H$ .

### 2.1.6 Normal Core of a subgroup

- 

$$H_G = \bigcap_{g \in G} gHg^{-1}$$

- Equivalently,  $H_G = \langle N : N \trianglelefteq G \text{ \& } N \leq H \rangle$ 
  - Largest normal subgroup that contains  $H$
- Equivalently,  $H_G = \ker \psi$  where  $\psi : G \rightarrow \text{Sym}(G/H)$ ;  $g \sim (xH) = (gx)H$
- Facts:
  - $H_G \trianglelefteq G$  and is an idempotent operation

### 2.1.7 Normal Closure of a subgroup

- $H^G = \{gHg^{-1} : g \in G\}$
- Equivalently,

$$H^G = \bigcap \{N : H \leq N \trianglelefteq G\}$$

- (The smallest normal subgroup of  $G$  containing  $H$ )

### 2.1.8 Group Action of a group on a set

- Given as a function

$$\phi : G \times X \rightarrow X (g, x) \mapsto g \sim x$$

which gives rise to a function

$$\phi_g : X \rightarrow X x \mapsto g \sim x$$

(which is a bijection) where  $\sim$  denotes a group element acting on a set element, and  $\forall x \in X$ ,

- $e \sim x = x$
- $(gh) \sim x = g \sim (h \sim x)$

- Equivalently, a function

$$\psi : G \rightarrow \text{Sym}(X) g \mapsto \phi_g$$

–

$$\ker \psi = \bigcap_{x \in X} G_x$$

(intersection of all stabilizers)

- Interesting actions:

- Left multiplication of  $G$  on  $G$ :

$$\phi : G \rightarrow G \rightarrow G \quad g \mapsto \phi_g : G \rightarrow G \quad h \mapsto gh$$

$$* \mathcal{O}_x = G \text{ (transitive)}$$

$$* G_x = e$$

- $G$  acting via conjugation on itself:

$$\phi : G \rightarrow G \rightarrow G \quad g \mapsto \psi_g : G \rightarrow G \quad h \mapsto ghg^{-1}$$

$$* \text{ A common notation is } x^g = g^{-1}xg \text{ which obeys } (x^g)^h = x^{gh}$$

$$* \mathcal{O}_x = [x] \text{ (Conjugacy classes, so not generally transitive)}$$

$$* G_x = \{g \in G : gxg^{-1} = x\} = C_G(x)$$

- $G$  acting on  $S = \{H : H \leq G\}$  via conjugation:

\*

$$\phi : G \rightarrow S \rightarrow S \quad g \mapsto \psi_g : S \rightarrow S \quad H \mapsto gHg^{-1}$$

$$* \mathcal{O}_H = [H] = \{gHg^{-1} : g \in G\}, \text{ conjugate subgroups of } H$$

$$* G_x = N_G(H) = \{g \in G : gHg^{-1} = H\}$$

### 2.1.9 Transitive group actions

- $\forall x, y \in X, \exists g \in G : g \sim x = y$
- Equivalent, actions with a single orbit

### 2.1.10 Orbit of a set element

$$\mathcal{O}_x = \{g \sim x : x \in X\} = \bigcup_{g \in G} \{g \sim x\}$$

- The set of all orbits is denoted  $X/G$  or  $X_G = \{\mathcal{O}_x : x \in X\}$
- Partitions  $X$  according to the equivalence relation  $x \cong y \iff \exists g \in G : g \sim x = y$
- $G$  acts transitively on  $X$  when restricted to any single orbit

### 2.1.11 Stabilizer of a set element

- $G_x = \{g \in G : g \sim x = x\}$
- Facts:
  - $G_x \leq G$ , not usually normal
  - $x, y \in \mathcal{O}_x \Rightarrow G_x$  is conjugate to  $G_y$

### 2.1.12 Automorphisms of a group

- $\text{Aut}(G) = \{\phi : G \rightarrow G : \phi \text{ is an isomorphism}\}$

### 2.1.13 Inner Automorphisms of a group

- $\text{Inn}(G) = \{\phi_g \in \text{Aut}(G) : \phi_g(x) = gxg^{-1}\}$
- Also consider the map

$$\psi : G \rightarrow \text{Aut}(G) \quad g \mapsto (\lambda : x \mapsto gxg^{-1})$$

Then  $\text{im}\psi = \text{Inn}(G)$ ,  $\ker\psi = Z(G)$

- Facts:
  - $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$
  - $\text{Inn}(G) \cong G/Z(G)$

### 2.1.14 Outer Automorphisms of a group

- $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$

### 2.1.15 Conjugacy Class of an element

•

$$[a] = \{gag^{-1} : g \in G\} = \bigcup_{g \in G} \{gag^{-1}\}$$

- Equivalently,  $[a] = \mathcal{O}_a$  under  $G$  acting on itself via conjugation
- Facts:
  - Equivalence relation, partitions the group
  - $|[a]|$  divides  $|G|$
  - $a \in Z(G) \Rightarrow [a] = \{a\}$

### 2.1.16 Characteristic subgroup

- $H \text{ char } G \iff \forall \phi \in \text{Aut}(G), \phi(H) = H$ 
  - i.e.,  $H$  is fixed by all automorphisms of  $G$ .

### 2.1.17 Simple group

- $G$  is simple  $\iff H \trianglelefteq G \Rightarrow H = e$  or  $G$ 
  - No non-trivial normal subgroups

### 2.1.18 Commutator of an element, or of subgroups

- $[g, h] = ghg^{-1}h^{-1}$
- $[G, H] = \langle [g, h] : g \in G, h \in H \rangle$  (Subgroup generated by commutators)

## 2.2 Structural Results

- Cyclic  $\Rightarrow$  abelian
- $G/Z(G)$  cyclic  $\Rightarrow G$  is abelian
- Intersections of subgroups are also subgroups

### 2.2.1 Isomorphisms Theorems

#### First Isomorphism Theorem

- Conditions:
  - $\phi : G \rightarrow G'$  is a homomorphism.
- Result:
  - $\ker \phi \trianglelefteq G$
  - $\text{im} \phi \leq G'$
  - $G/\ker \phi \cong \text{im} \phi$ .
- Corollaries:
  - $\ker \phi = e \Rightarrow G \cong G'$

#### Second Isomorphism Theorem

- Conditions:
  - $N \trianglelefteq G, H \leq G$
- Results:
  - $HN \leq G$
  - $N \cap H \trianglelefteq H$
  -

$$\frac{H}{H \cap N} \cong \frac{HN}{N}$$

- Corollaries:
  - (Weaker) Relaxing  $N \trianglelefteq G$  to  $H \subseteq N(N)$  yields
    - \*  $N \cap H \subseteq G$  (Not normal)
    - \*  $N \cap H \trianglelefteq H$

#### Third Isomorphism Theorem

- Conditions:
  - $N \trianglelefteq G, N \leq A \leq G$
- Results:
  - $A/N \leq G/N$ 
    - \* Every subgroup of  $G/N$  is of this form for *some* such  $A$
  -

$$\frac{G/N}{A/N} \cong \frac{G}{A}$$

\* Cancel the  $N$ !

- Corollaries:
  - $A \trianglelefteq G \Rightarrow A/N \trianglelefteq G/N$ 
    - \* All normal subgroups of  $G/N$  are of this form for some  $A$ .

### 2.3 Misc Results

- $G/N$  is abelian  $\iff [G, G] \leq N$
- $HK$  is not always a subgroup - see conditions in 2nd Isomorphism theorem'
- $H \trianglelefteq G, K \trianglelefteq G$  and  $H \cap K = e \Rightarrow hk = kh \forall h \in H, \in K$ 
  - Normal subgroups with trivial intersection commute
- $H \text{ char } G \Rightarrow H \trianglelefteq G$



- Characteristic is a strictly stronger condition than normality
- $H \text{ char } K \text{ char } G \Rightarrow H \text{ char } G$ 
  - Characteristic is transitive
- $H \leq G, K \trianglelefteq G, H \text{ char } K \Rightarrow H \trianglelefteq G$ 
  - i.e., normality is **not** transitive, strengthening normality to char gives “weak transitivity”
- Recognizing (Internal) Direct Products:  $H \leq G, K \leq G$ 
  - $H \cap K = e$
  - $\forall g \in G, \exists h \in H, k \in K : g = hk$
  - $H \trianglelefteq G, K \trianglelefteq G$ 
    - \* **OR** Every element in  $H$  commutes with every element in  $K$
- P Groups
  - $\bigcap P = O_P(G) \text{ char } G$ . And  $O_P(G) \trianglelefteq G$  as well.
  - $N \trianglelefteq G$  implies that  $P_N \leq N$  are of the form  $N \cap P_G$
  - $P \cap Q = e$

## 2.4 Numeric Results

### 2.4.1 Cauchy's Theorem

- For any  $p$  dividing  $|G|$ , there is a subgroup of order  $p$ .

### 2.4.2 Sylow Theorems: $|G| = p^k m$ where $p \nmid m$

- At least one Sylow- $p$  subgroup always exists:  $\exists P \leq G$  with  $|P| = p^k$
- All such subgroups are conjugate:  $\forall P, P', \exists g \in G : gPg^{-1} = P'$
- $n_p$  satisfies:
  - $n_p$  divides  $m = [G : P]$
  - $n_p \equiv 1 \pmod{p}$
  - $n_p = [G : N_G(P)]$  (Not as useful)
- Every  $p$ -subgroup of  $G$  is a  $p$ -subgroup of  $P$  (i.e.  $P$  is maximal and contains all subgroups of order  $p^l$  with  $l \leq k$ )

### 2.4.3 Orbit-stabilizer Theorem

- Given a group action,  $G/G_x \cong \mathcal{O}_x$
- Gives the numeric result  $|\mathcal{O}_x| = |G/G_x| = [G : G_x] = \frac{|G|}{|G_x|}$
- Also useful in the form  $|G| = |\mathcal{O}_x| |G_x|$
- Proof:
  - Use the map

$$\phi : G \rightarrow Xg \mapsto g \sim x$$

Where  $\text{im}\phi = \mathcal{O}_x$  and  $\ker\phi = G_x$ .

#### 2.4.4 Burnside's Lemma

•

$$|X_G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

- $|X_G|$  is the number of orbits
- $X^g = \{x \in X : g \sim x = x\}$

#### 2.4.5 The class equation

•

$$|G| = |Z(G)| + \sum_{a \in A} [G : C_G(a)]$$

- Where  $A = \{a_1, a_2, \dots, a_n : a_1 \in [a_1], a_2 \in [a_2], \dots\}$  is a set containing one element from each conjugacy class
- $[G : C_G(a)]$  is the number of elements in  $[a]$
- Each element in  $Z(G)$  has a singleton conjugacy class

#### 2.4.6 General facts

- $|G| = p \Rightarrow G$  is cyclic
- $|G| = p^e \Rightarrow Z(G) \neq e$
- $|G| = p^e$  (P-groups)
  - $Z(G) \neq \{e\}$  (Use class equation)
- $|G| = p$ 
  - Always cyclic
    - \* Proof: Any nontrivial cyclic subgroup's order is  $> 1$  and divides  $p$ , so equals  $p$ .
- $|G| = p^2$ 
  - Always abelian
    - \* Proof:  $|G/Z(G)| = 1, p$ . If  $p$ , it's cyclic, and  $G$  is abelian. Otherwise it's 1, so  $G = Z(G)$ .
  - Two possibilities:
    - \*  $Z_{p^2}$  (cyclic)
    - \*  $Z_p \times Z_p$
- $|G| = pq$ 
  - $p \nmid q-1$  ( $q \not\equiv 1 \pmod p$ ):
    - \* One possibility:
      - $G \cong Z_{pq}$  (cyclic)
    - \* Facts:
      - $\exists P \trianglelefteq G$  (A Sylow- $P$  subgroup)
  - $p$  divides  $q-1$  ( $q \equiv 1 \pmod p$ ):
    - \* Two possibilities:

- $G \cong Z_{pq}$  (cyclic)
- $G \cong Z_q \rtimes Z_p$
- Never simple
- $|G| = p^2q$ 
  - $\exists P \trianglelefteq G$  (A Sylow- $P$  subgroup)
- $|G| = p_1p_2p_3$  (distinct)
  - Not simple

## 2.5 Common Groups

### 2.5.1 $S_3$

$$S_3 = \langle (12), (23), (13) \rangle$$

- $Z(S_3) = e$
- $\text{Aut}(S_3) = \text{Inn}(S_3)$ , since

$$Z(G) = e = \ker \psi \Rightarrow \text{Out}(S_3) = \text{Inn}(S_3) \Rightarrow \text{Aut}(S_3) \cong S_3$$

### 2.5.2 $S_n$

$$S_n, n \geq 4$$

- $Z(S_n) = e$ 
  - Let  $\sigma(a) = b$ , choose  $\tau = (bc)$  so  $\tau\sigma(a) = \tau(b) = c \neq b = \sigma(a) = \sigma\tau(a)$
- Conjugacy classes are determined entirely by cycle structure
  - There are exactly  $p(n)$  of them (partition function)
- Disjoint cycles commute
- $\sigma \circ (a_1 \cdots a_k) \circ \sigma^{-1} = (\sigma(a_1), \cdots \sigma(a_k))$
- Every element is a product of disjoint cycles
- Every element is a product of transpositions
  - A cycle of length  $k$  can be written as  $k - 1$  transpositions
  - Parity of the cycle equals the parity of  $k - 1$ .
- The order of an element is the lcm of the size of the cycles.

### 2.5.3 $A_n$

- Simple for  $n \geq 5$
- Index 2 in  $S_n$ , so  $A_n \trianglelefteq S_n$

### 2.5.4 $D_n$

- $\langle a, b \mid a^n = b^2 = 1, bab^{-1} = a^{-1} \rangle \cong \langle r, s \rangle$
- $D_n/N$  is always another dihedral group for any  $N \trianglelefteq D_n$
- All subgroups:
  - $\langle r^d \rangle \cong Z_{n/d}$  where  $d$  divides  $n$  (index  $2d$ )
  - $\langle r^d, r^i s \rangle \cong D_{n/d}$  where  $d$  divides  $n$  and  $0 \leq i \leq d - 1$  (index  $d$ )

\* All dihedral

## 3 Rings

### 3.1 Facts about ideals:

- Intersections, products, and sums of ideals are ideals
- Not necessarily unions
- Every ring has proper maximal ideals
  - Apply Z.L. to  $\{I \trianglelefteq R : I \neq R\}$
- Every proper ideal is contained in a maximal ideal

### 3.2 Maximal ideals

$I \trianglelefteq R$  maximal if  $\nexists J \trianglelefteq R : I \subset J \subset R$

- Every nonzero ring has a maximal ideal (Krull's Theorem)
- $R$  commutative  $\implies R/I$  a field
- Union of maximal ideals  $= R - R^\times$
- $(X - a) \trianglelefteq R[X]$  is maximal for  $a \in R$

### 3.3 Prime ideals

$I \trianglelefteq R$  prime when  $pq \in I \implies p \in I \vee q \in I$

- $I$  prime  $\iff R/I$  an integral domain,
- (maximal  $\implies$  prime)
- $\text{rad}(I^n) = I$

### 3.4 Radicals

$I \trianglelefteq R$  radical when  $\forall a \in R, a^n \in I \implies a \in I$

•

$$\text{nilrad}(I) = \bigcap P$$

such that

$$P \trianglelefteq R$$

prime

- $\text{rad}(I) = \{x \in R \mid \exists n : x^n \in I\}$ 
  - $\text{rad}(0) = \text{nilrad}(R)$
  - $\text{rad}(IJ) = \text{rad}(I) \cap \text{rad}(J)$
  -

$$\text{rad}(I) = \bigcap J$$

such that  $I \subset J, J$  prime (i.e. intersection of all prime ideals containing  $I$ )

–