Harold's Abstract Algebra
Cheat Sheet
21 October 2022
DRAFT

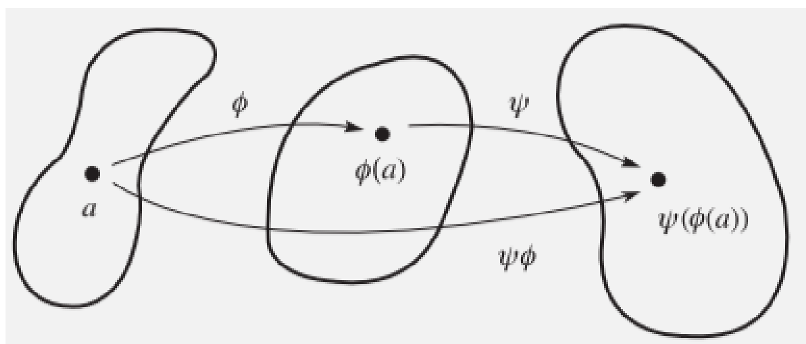
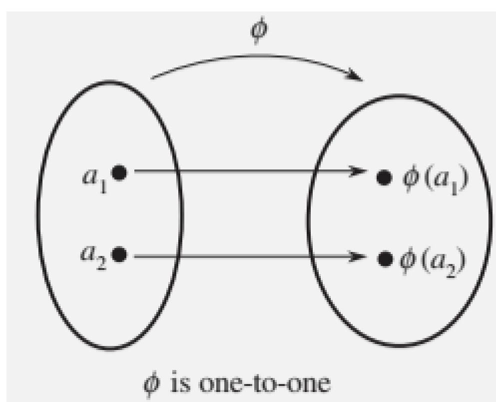
Symbols

Symbol	Name / Definition	Symbol	Name / Definition
∅	**Empty** set, set with no members	R_0, R_{90}, R_{180}, R_{270}	Rotation
ℕ	**Natural** numbers	$R_{360/n}$	Cyclic Rotation
ℤ	**Integers** (Zahlen)	H, V, D, D'	Flip (horizontal, vertical, diagonal)
ℚ	**Rational** numbers	⟨a⟩	The set $\{a^n \mid n \in \mathbb{Z}\}$ under • (na if +)
ℝ	**Real** numbers	$\begin{bmatrix} A & B \\ C & D \end{bmatrix}^{-1}$	2x2 Matrix Inverse
ℂ	**Complex** numbers	Z_n	Group of integers modulo n
F*	Nonzero Field	Z_p	Z_n where p a prime
⊆	Is a subset of	mod	Modulus arithmetic
∈	Is an element of	GL(2, F)	General Linear Group of 2x2 matrices over the field F
∞	Infinity	g^n	The group operation on g n times
°	Degrees	|G|	Order of a Group
≤, ≠, ≥	Inequalities	|g|	Order of an Element
•, ·	Multiply	gcd (a, b)	Greatest Common Divisor
÷	Division	lcm (a, b)	Least Common Multiple
a | b	a divides b		
a^{-1}	Inverse		
<tab>			

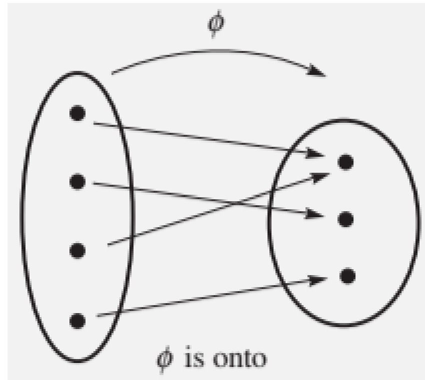
Ch. 0: Preliminaries

Definition	Description
Well Ordering Principle	Every nonempty set of positive integers contains a smallest member.
Theorem 0.1: Division Algorithm	Let a and b be integers with b > 0. Then there exist unique integers q and r with the property that a = bq + r, where 0 ≤ r < b. Example: For a = 17 and b = 5, the division algorithm gives 17 = 5 · 3 + 2. Here q = 3 and r = 2.
Greatest Common Divisor (GCD)	$gcd\ (x, y) = p_1^{min\{\alpha_1,\beta_1\}} \cdot p_2^{min\{\alpha_2,\beta_2\}} \cdot p_k^{min\{\alpha_k,\beta_k\}}$ Largest positive integer that is a factor of both x and y. Think Intersection (∩) of α_i, β_i.
	The greatest common divisor of two nonzero integers a and b is the largest of all common divisors of a and b. We denote this integer by **gcd (a, b)**.
Relatively Prime Integers	When gcd (a, b) = 1, we say a and b are relatively prime.
Theorem 0.2: GCD Is a Linear Combination	For any nonzero integers a and b, there exist integers s and t such that gcd (a, b) = as + bt. Moreover, gcd(a, b) is the smallest positive integer of the form as + bt.
Corollary	If a and b are relatively prime, then there exist integers s and t such that as + bt = 1. Example: gcd (4, 15) = 1 where 4 and 15 are relatively prime and 4 · 4 + 15(-1) = 1.
Euclid's Lemma p | ab Implies p | a or p | b	If p is a prime that divides ab, then p divides a or p divides b.
Theorem 0.3: Fundamental Theorem of Arithmetic	Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear. That is, if n = $p_1p_2 \ldots p_r$ and n = $q_1q_2 \ldots q_s$, where the p's and q's are primes, then r = s and, after renumbering the q's, we have $p_i = q_i$ for all i.
Least Common Multiple (LCM)	$lcm\ (x, y) = p_1^{max\{\alpha_1,\beta_1\}} \cdot p_2^{max\{\alpha_2,\beta_2\}} \cdot p_k^{max\{\alpha_k,\beta_k\}}$ Smallest positive integer that is an integer multiple of both x and y. Think Union (∪) of α_i, β_i.
	The least common multiple of two nonzero integers a and b is the smallest positive integer that is a multiple of both a and b. We will denote this integer by **lcm (a, b)**. Example: lcm (4, 6) = 12
Computing ab mod n or (a + b) mod n	Let n be a fixed positive integer greater than 1. If a mod n = a' and b mod n = b', then (a + b) mod n = (a' + b') mod n (ab) mod n = (a'b') mod n

Logic Gates	A logic gate is a device that accepts as inputs two possible states (on or off) and produces one output (on or off). This can be conveniently modeled using 0 and 1 and modulo 2 arithmetic. x AND y xy x OR y x + y + xy x XOR y x + y MAJ(x, y, z) xz + xy + yz.
Theorem 0.4: **Properties of Complex Numbers**	1. Closure under addition: (a + bi) + (c + di) = (a + c) + (b + d)i 2. Closure under multiplication: (a + bi) (c + di) = (ac) + (ad)i + (bc)i + (bd)i^2 = (ac - bd) + (ad + bc)i 3. Closure under division (c + di ≠ 0): $\frac{(a+bi)}{(c+di)} = \frac{(a+bi)}{(c+di)} \bullet \frac{(c-di)}{(c-di)}$ $= \frac{(ac+bd)+(bc-ad)i}{c^2+d^2}$ $= \frac{(ac+bd)}{c^2+d^2} + \frac{(bc-ad)}{c^2+d^2}i$ 4. Complex conjugation: (a + bi) (a - bi) = $a^2 + b^2$ 5. Inverses: For every nonzero complex number a + bi there is a complex number c + di such that (a + bi) (c + di) = 1 (That is, $(a + bi)^{-1}$ exists in C). 6. Powers: For every complex number a + bi = r(cos θ + i sin θ) and every positive integer n, we have $(a + bi)^n = (r(\cos\theta + i\sin\theta))^n = r^n (\cos n\theta + i \sin n\theta)$. 7. n^{th}-roots of a + bi: For any positive integer n the n distinct n^{th} roots of a + bi = r(cos θ + i sin θ) are $\sqrt[n]{r}\left(\cos\frac{\theta+2\pi k}{n} + i\sin\frac{\theta+2\pi k}{n}\right)$ for k = 0, 1, …, n - 1.
Theorem 0.5: **First Principle of Mathematical Induction**	Let S be a set of integers containing a. Suppose S has the property that whenever some integer n ≥ a belongs to S, then the integer n + 1 also belongs to S. Then, S contains every integer greater than or equal to a.
DeMoivre's Theorem	$(\cos\theta + i \sin\theta)^n = (\cos n\theta + i \sin n\theta)$
Theorem 0.6: **Second Principle of Mathematical Induction**	Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to a belongs to S. Then, S contains every integer greater than or equal to a.

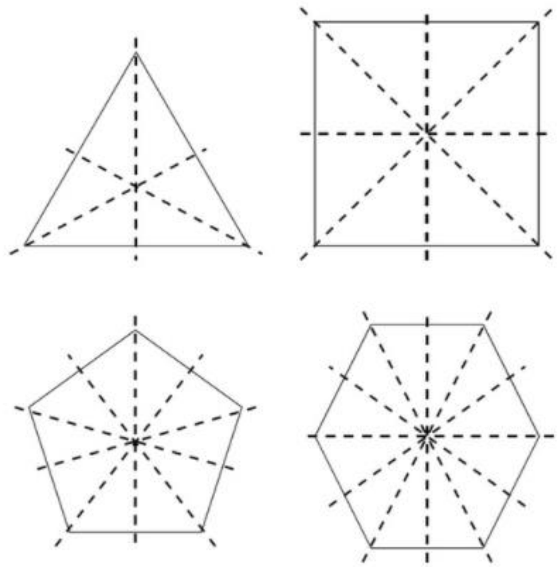
Equivalence Relation	An equivalence relation on a set S is a set R of ordered pairs of elements of S such that 1. $(a, a) \in R$ for all $a \in S$ (reflexive property). 2. $(a, b) \in R$ implies $(b, a) \in R$ (symmetric property). 3. $(a, b) \in R$ and $(b, c) \in R$ imply $(a, c) \in R$ (transitive property). NOTE: It is customary to write aRb instead of $(a, b) \in R$.
Theorem 0.7: Equivalence Classes Partition	The equivalence classes of an equivalence relation on a set S constitute a partition of S. Conversely, for any partition P of S, there is an equivalence relation on S whose equivalence classes are the elements of P.
Function (Mapping)	A function (or mapping) f from a set A to a set B is a rule that assigns to each element a of A exactly one element b of B. The set A is called the domain of f, and B is called the range of f. If f assigns b to a, then b is called the image of a under f. The subset of B comprising all the images of elements of A is called the image of A under f.
Composition of Functions	Let $f: A \rightarrow B$ and $g: B \rightarrow C$. The composition gf is the mapping from A to C defined by $(gf)(a) = g(f(a))$ for all a in A.  $(f \circ g)(x) = f(g(x))$
One-to-One Function	A function f from a set A is called one-to-one if for every $a_1, a_2 \in A$, $f(a_1) = f(a_2)$ implies $a_1 = a_2$. 

<table>
<tr>
<td>Function from A onto B</td>
<td>A function f from a set A to a set B is said to be onto B if each element of B is the image of at least one element of A. In symbols, f: A → B is onto if for each b in B there is at least one a in A such that f(a) = b.


</td>
</tr>
<tr>
<td>Theorem 0.8:
Properties of Functions</td>
<td>Given functions f: A → B, g: B → C, and h: C → D, then
1. h(gf) = (hg)f (associativity).
2. If f and g are one-to-one, then gf is one-to-one.
3. If f and g are onto, then gf is onto.
4. If f is one-to-one and onto, then there is a function f^{-1} from B onto A such that $(f^{-1}f)(f) = f$ for all f in A and $(ff^{-1})(g) = g$ for all g in B.

<table>
<tr><th>Domain</th><th>Range</th><th>Rule</th><th>One-to-One</th><th>Onto</th></tr>
<tr><td>$\mathbf{Z}$</td><td>$\mathbf{Z}$</td><td>$x \to x^3$</td><td>Yes</td><td>No</td></tr>
<tr><td>$\mathbf{R}$</td><td>$\mathbf{R}$</td><td>$x \to x^3$</td><td>Yes</td><td>Yes</td></tr>
<tr><td>$\mathbf{Z}$</td><td>$\mathbf{N}$</td><td>$x \to |x|$</td><td>No</td><td>Yes</td></tr>
<tr><td>$\mathbf{Z}$</td><td>$\mathbf{Z}$</td><td>$x \to x^2$</td><td>No</td><td>No</td></tr>
</table></td>
</tr>
<tr>
<td>Cancellation Property</td>
<td>Suppose f, g, and h are functions. If fh = gh and h is one-to-one and onto, then f = g.</td>
</tr>
</table>

Ch. 1: Introduction to Groups

Definition	Description
Abelian	Commutative (ab = ba) Named after Niels Abel, Norwegian mathematician.
Non-Abelian	Not commutative (ab ≠ ba)
D_n: **Dihedral Groups**	D_n = *dihedral group of order 2n*. Dihedral = having or contained by two plane faces. Examples: D_3, D_4, D_5, D_6 
D_4: **Dihedral Group of Order 8**	D_4 (Square) The eight motions R_0, R_{90}, R_{180}, R_{270}, H, V, D, and D', together with the operation composition, form a mathematical system called the dihedral group of order 8 (the order of a group is the number of elements it contains). It is denoted by D_4.
Cayley Table	Operations table. All elements in the rows and columns, filled in with the operation results. Named after Arthur Cayley, English mathematician.
Cyclic Rotation Group of Order n	$\langle R_{360/n} \rangle$ Many objects and figures have rotational symmetry but not reflective symmetry. A symmetry group consisting of the rotational symmetries of 0°, 360°/n, 2(360°)/n, ..., (n - 1)360°/n, and no other symmetries.

Ch. 2: Groups

Theorem / Definition	Description
Binary Operation	Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G. (Closure)
Group	Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element **in** G (closure) denoted by ab. We say G is a *group* under this operation if the following three properties are satisfied. 1. *Associativity*. The operation is associative; that is, (ab)c = a(bc) for all a, b, c in G. 2. *Identity*. There is an element e (called the *identity*) in G such that ae = ea = a for all a in G. 3. *Inverses*. For each element a in G, there is an element b in G (called an *inverse* of a) such that ab = ba = e.
Algebraic Systems	Sets with one or more binary operations.
Abstract Algebra	The goal of abstract algebra is to discover truths about algebraic systems that are independent of the specific nature of the operations. All one knows or needs to know is that these operations, whatever they may be, have certain properties. We then seek to deduce consequences of these properties.
GL(2, F)	*General Linear Group* of 2x2 matrices over the field F. Non-Abelian.
SL(2, F)	*Special Linear Group* of 2x2 matrices over the field F with determinant 1. Non-Abelian.
Z_n	Group of integers modulo n. $Z_n = \{0, 1, ..., n - 1\}$ for $n \geq 1$. Implies the operation of **addition**.
U(n)	The set of all positive integers less than n and relatively prime to n under the operation of **multiplication** modulo n. $U(n) = \{a \in Z_n \mid a < n \text{ and } \gcd(a, n) = 1\}$. If n is a prime, then U(n) = {0, 1, ..., n - 1}.
U(n) Examples	U(2) = {1, 2} prime U(3) = {1, 2, 3} prime U(4) = {1, 3} U(5) = {1, 2, 3, 4} prime U(6) = {1, 3, 5} U(7) = {1, 2, 3, 4, 5, 6} prime U(8) = {1, 3, 5, 7} U(10) = {1, 3, 7, 9} U(15)={1, 2, 4, 7, 8, 11, 13, 14} U(18) = {1, 5, 7, 11, 13, 17}

Theorem 2.1: Uniqueness of the Identity	In a group G, there is only one identity element.
Theorem 2.2: Cancellation	In a group G, the right and left cancellation laws hold; that is, ba = ca implies b = c, and ab = ac implies b = c.
Theorem 2.3: Uniqueness of Inverses	For each element a in a group G, there is a unique **element** b in G such that ab = ba = e.
g^n	Product: g g g g … g (n factors) Sum: g+g+g+g+…+g (n factors) g^0 = e or identity If g is negative: $g^n = (g^{-1})^{\lvert n \rvert}$
Multiplicative Group	a• b or ab — Multiplication e or 1 — Identity or one a^{-1} — Multiplicative inverse of a a^n — Power of a ab^{-1} — Quotient
Additive Group	a + b — Addition 0 — Identity or zero -a — Additive inverse of a na — Multiple of a a - b — Difference
Theorem 2.4: Socks–Shoes Property	For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.
Division Algorithm	$k = qn + r$ with $0 \le r < n$. q is the quotient; r is the remainder.

Table 2.1 Summary of Group Examples (F can be any of Q, R, C, or Z_p; L is a reflection)

Group	Operation	Identity	Form of Element	Inverse	Abelian
Z	Addition	0	k	$-k$	Yes
Q^+	Multiplication	1	m/n, $m, n > 0$	n/m	Yes
Z_n	Addition mod n	0	k	$n - k$	Yes
$\mathbf{R}^*$	Multiplication	1	x	$1/x$	Yes
$\mathbf{C}^*$	Multiplication	1	$a + bi$	$\frac{1}{a^2 + b^2}a - \frac{1}{a^2 - b^2}bi$	Yes
$GL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc \neq 0$	$\begin{bmatrix} \frac{d}{ad - bc} & \frac{-b}{ad - bc} \\ \frac{-c}{ad - bc} & \frac{a}{ad - bc} \end{bmatrix}$	No
$U(n)$	Multiplication mod n	1	k, $\gcd(k, n) = 1$	Solution to $kx \bmod n = 1$	Yes
$\mathbf{R}^n$	Componentwise addition	$(0, 0, \ldots, 0)$	$(a_1, a_2, \ldots, a_n)$	$(-a_1, -a_2, \ldots, -a_n)$	Yes
$SL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc = 1$	$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$	No
D_n	Composition	R_0	R_α, L	$R_{360 - \alpha}$, L	No

Ch. 3: Finite Groups; Subgroups

Axiom / Theorem / Lemma / Definition	Description
Order of a Group (|G|)	The number of elements of a group (finite or infinite) is called its *order*. We will use |G| to denote the order of G.
Order of an Element (|g|)	The *order* of an element g in a group G is the smallest positive integer n such that $g^n = e$. (In additive notation, this would be ng = 0.) If no such integer exists, we say that g has *infinite order*. The order of an element g is denoted by |g|.
Subgroup	If a <u>subset</u> H of a group G is itself a group under the operation of G, we say that H is a *subgroup* of G. $H \leq G$
Proper Subgroup	$H < G$ means "H is a proper subgroup of G".
Trivial Subgroup	The *trivial subgroup* of any group is the subgroup {e} consisting of just the identity element.
Modular Arithmetic	Google: To compute 13^4 mod 15, just type in the search box: "13ˆ4 mod 15"
Theorem 3.1: **One-Step Subgroup Test**	Let G be a group and H a nonempty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G. (In additive notation, if a - b is in H whenever a and b are in H, then H is a subgroup of G.) 1. Identify the property P that distinguishes the elements of H; that is, identify a defining condition. 2. Prove that the identity has property P. (This verifies that H is nonempty.) 3. Assume that two elements a and b have property P. 4. Use the assumption that a and b have property P to show that ab^{-1} has property P.
Theorem 3.2: **Two-Step Subgroup Test**	Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H (H is closed under the operation), and a^{-1} is in H whenever a is in H (H is closed under taking inverses), then H is a subgroup of G.
Not a Subgroup	To guarantee that the subset is not a subgroup, show one: 1. Show that the <u>identity</u> is not in the set. 2. Exhibit an element of the set whose <u>inverse</u> is not in the set. 3. Exhibit two elements of the set whose <u>product</u> is not in the set.
Theorem 3.3: **Finite Subgroup Test**	Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

Cyclic Subgroup $\langle a\rangle$	The subgroup $\langle a\rangle$ is called the *cyclic subgroup of G generated by a*. $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$ under multiplication $\langle a\rangle = \{na \mid n \in \mathbb{Z}\}$ under addition
Cyclic Group	In the case that $G = \langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$, we say that G is *cyclic* and a is a *generator* of G. Cyclic Group if there is an element a in G such that $G = \{a^n \mid n \in \mathbb{Z}\}$. Element 'a' is called the *generator*. A cyclic group may have many generators.
Theorem 3.4: **$\langle a\rangle$ Is a Subgroup**	Let G be a group, and let a be any element of G. Then, $\langle a\rangle$ is a subgroup of G. Use $\langle a\rangle$ or <a>.
$\langle a\rangle$ Examples	<u>Under Addition:</u> $\langle 2\rangle = \{0, 2, 4, 6, \ldots, 2n, \ldots\}$ $\langle 2\rangle = Z_{20}\ \langle 8, 14\rangle = \{0, 2, 4, \ldots, 18\}$ $\langle 3\rangle = \{0, 3, 6, 9, \ldots, 3n, \ldots\}$ $U(10) = [1, 3, 7, 9] = \langle 3\rangle = \langle 7\rangle$ $Z_8 = \langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle = \{0, 1, 2, 3, 4, 5, 6, 7\}$ <u>Under Multiplication:</u> $\langle 3\rangle = \{3, 9, 7, 1\} = \{1, 3, 7, 9\}$ mod 10 $\langle 3\rangle = \{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{1, 3, 5, 9, 11, 13\}$ mod 14
Center of a Group	The *center*, Z(G), of a group G is the subset of elements in G that *commute* with every element of G. In symbols, $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}$. [The German word for center is Zentrum]
Theorem 3.5: **Center Is a Subgroup**	The center of a group G is a subgroup of G.
Centralizer of a in G	Let a be a fixed element of a group G. The *centralizer* of a in G, C(a), is the set of all elements in G that commute with a. In symbols, $C(a) = \{g \in G \mid ga = ag\}$.
Theorem 3.6: **C(a) Is a Subgroup**	For each a in a group G, the centralizer of a is a subgroup of G.

Ch. 4: Cyclic Groups

Axiom / Theorem / Lemma / Definition	Description
Cyclic Group	If there is an element a in G such that $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. Element a is called the *generator*.
Theorem 4.1: **Criterion for $a^i = a^j$**	Let G be a group, and let a belong to G. If a has **infinite order**, then $a^i = a^j$ if and only if $i = j$. If a has **finite order**, say, n, then $\langle a \rangle = \{e, a, a^2, ..., a^{n-1}\}$ and $a^i = a^j$ if and only if n divides *into* $i - j$ *evenly*.
Corollary 1: **$\|a\| = \|\langle a \rangle\|$**	For any group element a, $\|a\| = \|\langle a \rangle\|$.
Corollary 2: **$a^k = e$ Implies That $\|a\|$ Divides k**	Let G be a group and let a be an element of order n in G. If $a^k = e$, then n divides k.
Corollary 3: **Relationship between $\|ab\|$ and $\|a\|\|b\|$**	If a and b belong to a finite group and ab = ba, then $\|ab\|$ divides $\|a\|\|b\|$.
Implication of Theorem 4.1	<u>Finite Case:</u> Multiplication in $\langle a \rangle$ is addition modulo n. Example: If $(i + j) \bmod n = k$, then $a^i a^j = a^k = a^{(i + j) \bmod n}$. Multiplication in $\langle a \rangle$ works the same as addition in Z_n whenever $\|a\| = n$. <u>Infinite Case:</u> Multiplication in $\langle a \rangle$ is addition. Example: $a^i a^j = a^{i+j}$. Multiplication in $\langle a \rangle$ works the same as addition in Z.
Theorem 4.2: **$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $\|a^k\| = n/\gcd(n, k)$**	Let a be an element of **finite** order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $\|a^k\| = n/\gcd(n, k)$. The **greatest common divisor (GCD)** of two nonzero integers a and b is the greatest positive integer d such that d is a divisor of both a and b.
Corollary 1: **Orders of Elements in Finite Cyclic Groups**	In a finite cyclic group, the order of an element divides the order of the group.
Corollary 2: **Criterion for $\langle a^i \rangle = \langle a^j \rangle$ and $\|a^i\| = \|a^j\|$**	Let $\|a\| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$, and $\|a^i\| = \|a^j\|$ if and only if $\gcd(n, i) = \gcd(n, j)$.
Corollary 3: **Generators of Finite Cyclic Groups**	Let $\|a\| = n$. Then $\langle a \rangle = \langle a^j \rangle$ if and only if $\gcd(n, j) = 1$, and $\|a\| = \|\langle a^j \rangle\|$ if and only if $\gcd(n, j) = 1$. NOTE: $\gcd(n, j) = 1$ means n and j are relatively prime.
Corollary 4: **Generators of Z_n**	An integer k in Z_n is a generator of Z_n if and only if $\gcd(n, k) = 1$.

Theorem 4.3: **Fundamental Theorem of Cyclic Groups**	Every subgroup of a cyclic group is cyclic. Moreover, if $\|\langle a \rangle\| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k — namely, $\langle a^{n/k} \rangle$.
Corollary: **Subgroups of Z_n**	For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of Z_n of order k; moreover, these are the only subgroups of Z_n.
Theorem 4.4: **Number of Elements of Each Order in a Cyclic Group**	If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.
Corollary: **Number of Elements of Order d in a Finite Group**	In a finite group, the number of elements of order d is a multiple of $\phi(d)$.

Ch. 5: Permutation Groups

Axiom / Theorem / Lemma / Definition	Description

Ch. 6: Isomorphisms

Axiom / Theorem / Lemma / Definition	Description

Ch. 7: Cosets and Lagrange's Theorem

Axiom / Theorem / Lemma / Definition	Description

Note: Skip Ch. 8

Ch. 9: Normal Subgroups and Factor Groups

Axiom / Theorem / Lemma / Definition	Description

Ch. 10: Group Homomorphisms

Axiom / Theorem / Lemma / Definition	Description

Ch. 11: Fundamental Theorem of Finite Abelian Groups

Axiom / Theorem / Lemma / Definition	Description

Ch. 12: Introduction to Rings

Axiom / Theorem / Lemma / Definition	Description

Sources:

- SNHU MAT 470 - Real Analysis, The Real Numbers and Real Analysis, Ethan D. Bloch, Springer New York, 2011.