Algebra Exam 3 Note Sheets

1.2 Binary Operations

Definitions:

Binary Operation:	A binary operation $*$ on set S is a function from $S \times S$ to S. We denote an output as $a*b$. Big Idea: Take 2 elements from S, (a, b) and the operation gives $a * b$, which is an element of S.
Commutative:	If $a * b = b * a$ for all $a, b \in S$.
Associative:	If $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.
Closed:	Suppose $*$ is a binary operation on S and $H \subset S$. We say H is closed under $*$ if for all $a, b \in H$, $a * b \in H$.
Identity:	There exists $e \in G$ such that for all $a \in G$, $a*e = e*a = a$.
Inverse:	For all $a \in G$, there exists $a' \in G$ such that $a*a' = a'*a = e$.

Examples:

1. Let $L = \{n^2 \mid n \in \mathbb{N}\}$. Is L closed under $+$? No: $16 + 4 \notin L$.
2. Is L closed under $\cdot$? Yes. Let $a, b \in L$. There exists $n, m \in L$ such that $a = n^2$ and $b = m^2$. Then $a \cdot b = n^2 \cdot m^2 \implies a \cdot b = (nm)^2$. Since $n, m \in \mathbb{N}$, $a, b \in L$. Therefore, L is closed under $\cdot$.
3. For tables, calculations are made from the column element to the row element. Commutativity and associativity can be checked by testing all possible combinations.
4. Let $*$ be defined on $\mathbb{R}^+$ by letting $a * b = \frac{a+b}{ab}$.
   - Is $*$ commutative? *Sol.* $a*b = \frac{a+b}{ab} = \frac{b+a}{ba} = b*a$ because addition and multiplication on the real line are commutative.
   - Is $*$ associative? *Sol.* No. Counterexample: $(4*2)*3 = \frac{4+2}{8} * 3 = \ldots$.
   - Explain why $*$ does not define a binary operation on $\mathbb{R}$. *Sol.* Since $1, 0 \in \mathbb{R}$, $1 * 0 = \frac{1+0}{(1)0}$ is undefined, so the set is not closed.
   - Explain why $*$ does not define a binary operation on $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$. *Sol.* Since $-1, 1 \in \mathbb{R}^*$, $-1 * 1 = \frac{-1+1}{(-1)(1)} = 0$, which is not in $\mathbb{R}^*$, so it's not closed.
5. Consider the set of matrices $H = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}$. Show that $\langle \mathbb{C}, \cdot \rangle$ is isomorphic to $\langle H, \cdot \rangle$ using the map $\varphi(a + bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. *Solution:* 1-1: Let $\varphi(a + bi) = \varphi(c + di)$. Then, $\begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} c & -d \\ d & c \end{bmatrix}$, so that $a = c$ and $b = d$. Onto: If $\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in H$, then $\varphi(a + bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. So, φ is onto. Homomorphism: $\varphi(a + bi) \cdot \varphi(c + di) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac - bd & -(bc + ad) \\ bc + cd & ac - bd \end{bmatrix} = \varphi((ac - bd) + (ad + bc)i) = \varphi((a + bi) \cdot (c + di))$.

1.3 Isomorphisms

Definitions:

Isomorphism:	Let $\langle G, * \rangle$ and $\langle G', *' \rangle$ be 2 binary structures. We say they are *isomorphic* if there exists an function $\phi : G \to G'$ such that 1. ϕ is a bijection 2. ϕ preserves the operation $(\forall a, b \in G,\ \phi(a * b) = \phi(a) *' \phi(b))$.
One-to-One:	If $f(a) = f(b)$, then $a = b$.
Onto:	Let $f : X \to Y$. f is *onto* if for every $y \in Y$, there exists at least one $x \in X$ such that $f(x) = y$.

Examples:

1. $\langle \mathbb{Z}, + \rangle$ with $\phi : \mathbb{Z} \to 2\mathbb{Z}$ and $\langle 2\mathbb{Z}, + \rangle$ with $\phi(x) : 2x$. This is one-to-one (just draw a diagram and line them up to each other), and onto because every element in y has an x that is mapped to it. It's a homomorphism because $\phi(a + b) = 2(a + b) = 2a + 2b = \phi(a) + \phi(b)$.

To prove that two groups are not isomorphic, you must rely on *structural properties*. Consider the following examples to demonstrate structural property differences:

2. The sets $\mathbb{Z}$ and $\mathbb{Z}^+$ both have cardinality $\aleph_0$, and there are lots of one-to-one functions mapping $\mathbb{Z}$ onto $\mathbb{Z}^+$. However, the binary structures $\langle \mathbb{Z}, \cdot \rangle$ and $\langle \mathbb{Z}^+, \cdot \rangle$, where $\cdot$ is the usual multiplication, are not isomorphic. In $\langle \mathbb{Z}, \cdot \rangle$, there are two elements x such that $x \cdot x = x$, namely 0 and 1. However, in $\langle \mathbb{Z}^+, \cdot \rangle$, there is only the single element 1.
3. The binary structures $\langle \mathbb{C}, \cdot \rangle$ and $\langle \mathbb{R}, \cdot \rangle$ under the usual multiplication are not isomorphic. (It can be shown that $\mathbb{C}$ and $\mathbb{R}$ have the same cardinality.) The equation $x \cdot x = c$ has a solution x for all $c \in \mathbb{C}$, but $x \cdot x = -1$ has no solution in $\mathbb{R}$.

These are a list of possible structural and nonstructural properties:

Structural Properites

1. The set has 4 elements.
2. The operation is commutative.
3. $x * x = x$ for all $x \in S$.
4. The equation $a * x = b$ has a solution x in S for all $a, b \in S$

Nonstructural Properties

1. The number 4 is an element.
2. The operation is called "addition."
3. The elements of S are matrices.
4. S is a subset of $\mathbb{C}$.

1.4 Groups

Definitions:

A *group* $\langle G, * \rangle$ is a set G closed under a binary operation $*$ such that there is an inverse, an identity element, and the associative property is upheld.

Examples:

Let $*$ be defined on $\mathbb{Q}^+$ as $a * b = \frac{ab}{2}$. Show this is a group:

- **Associativity:** Let $a, b, c \in \mathbb{Q}^+$. $(a*b)*c = \frac{ab}{2} * c = \frac{abc}{4} = \frac{2(bc/2)}{2} = a * \frac{bc}{2} = a * (b * c)$.
- **Identity:** $a * e = a \implies e = 2$.
- **Inverses:** $a * a' = 2 \implies \frac{aa'}{2} = 2 \implies aa' = 4 \implies a' = \frac{4}{a} \implies a * \frac{4}{a} = \frac{a(4/a)}{2} = 2$. So, the identity is $a' = \frac{4}{a}$, and this exists in the group.

1.5 Subgroups

Definitions:

Subgroup: Let G be a group, where $H \subseteq G$. H is called a *subgroup* of G if:

1. H is closed under the operation.
2. Identity element belongs to H.
3. Each element of H must have its inverse in H.

Note: For finding subgroups of some modulo integer set, just use the divisors of the set.

Examples:

1. Determine whether the group consisting of the $n \times n$ matrices with determinant -1 or 1 is a subgroup of $GL(n, \mathbb{R})$. Let H be the set of all $n \times n$ matrices with determinant -1 or 1. We will show that H is a subgroup of $GL(n, \mathbb{R})$ by verifying the subgroup criterion:
   - **Identity:** The identity matrix I_n has a determinant of 1, so $I_n \in H$.
   - **Closure:** Let $A, B \in H$. Then $\det(A) = \pm 1$ and $\det(B) = \pm 1$. The determinant of the product AB is given by $\det(AB) = \det(A)\det(B) = (\pm 1)(\pm 1) = \pm 1$. Thus, $AB \in H$.
   - **Inverses:** Let $A \in H$. Then $\det(A) = \pm 1$. The determinant of the inverse A^{-1} is given by $\det(A^{-1}) = \frac{1}{\det(A)} = \pm 1$.. Thus, $A^{-1} \in H$.
2. When drawing subgroup diagrams for a cyclic group (e.g., $\mathbb{Z}_{30}$), list out the divisors (e.g., 1, 2, 3, 5, 6, 10, 15, 0) and have $\mathbb{Z}_{30}$ at the top, and $\langle 0 \rangle$ at the bottom.

1.6 Cyclic Groups

Definitions:

Cyclic: A group is *cyclic* if there exists an element $a \in G$ such that $G = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$. We call the element $a \in G$ a generator.

Order: For any $b \in G$, $\langle b \rangle$ is a cyclic subgroup. The *order* of element b is the cardinality of b.

Relatively Prime: If two integers are *relatively prime*, then their $\gcd(r, s) = 1$. Thus, there exists $n, m \in \mathbb{Z}$ such that $nr + ms = 1$.

The Division Algorithm for $\mathbb{Z}$: Let m be a positive integer, and n be any integer. Then there exists unique q and r such that $n = m \cdot q + r$ with $0 \leq r < m$ (where q is the quotient, r is the remainder). Idea: $n = 42$, $m = 8$, $42 = 8(5) + 2$ and $n = -42$, $m = 8$, $-42 = 8(-6) + 6$.

Proof. On a number line where we have 0, m, $2m$, etc. n is either a multiple of m or it falls between two multiples of m. Let q be the largest integer such that $qm \leq n$. Then $r = n - qm$. Hence, $0 \leq r < m$. □

Theorems:

Theorem 1: Every subgroup of a cyclic group is cyclic.

Theorem 2: Let G be a cyclic subgroup. If G is infinite, then $G \simeq \mathbb{Z}$. If G is finite, with order n, then $G \simeq \mathbb{Z}_n$. ($\simeq$ is equivalence relation.)

Theorem 3: Let G be a cyclic group with n elements with generator a and $b = a^s$. Then b generates a cyclic subgroup of G of which contains $\frac{n}{d}$ elements where $d = \gcd(s, n)$. Also $\langle a^s \rangle = \langle a^t \rangle \iff \gcd(s, n) = \gcd(t, n)$.

1.7 Generating Sets

Properties of Cayley Digraphs:

1. The graph is always connected.
2. At most, 1 arc can go from 1 vertex to another.
3. Each vertex has exactly 1 type of each arc starting at the vertex and ending at the vertex.
4. If two sequences of arc types starting at one vertex end at the same place, then the same two sequences starting at a common vertex will end at the same place.

Any digraph that has these properties is a group.

If asked to draw a Cayley digraph, start with the identity element, and then use the specified generating elements to build the graph from there. For example, take $\mathbb{Z}_8$ with the generator set $\{2, 5\}$. You would start with 0, but then have different lines. One for 2, ℓ_1, and one for 5, ℓ_2. $\ell_1 : 0 \to 2 \to 4 \to 6 \to 0$, $\ell_2 : 0 \to 5 \to 2 \to 7 \to 4 \to 1 \to 6 \to 3 \to 0$. Then, connect each line to each other. In other words, every vertex should have 4 lines going through it.

2.8 Groups of Permutations

Definitions:

- A *permutation* of a set is a bijection of that set onto itself.
  - The permutations of a set form a group with function composition as the binary operation. So, $\sigma\tau$ is read right to left. For a multiplication table, it is read top first.
  - For the set $\{1, 2, \ldots, n\}$, we call the group of permutations S_n, where $|S_n| = n!$.
- Let $f\colon A \to B$ be a function and H be a subset of A. Then $f(H) = \{f(x) \in H\}$ is called the *image of H under f*.
- **Cayley's Theorem:** Every group is isomorphic to a group of permutations (a subgroup of S_n where $n =$ order of the group)
- **Lemma:** If G and G' are groups and $\varphi\colon G \to G'$ is a 1-1 homomorphism, then $\varphi(G)$ is a subgroup of G' and G is isomorphic to $\varphi(G)$.

Examples:

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

2.9 Orbits, Cycles, and the Alt. Groups

Definitions:

- Let A be a set and $\sigma \in S_A$. For a fixed $a \in A$, the *orbit* of a under σ is $\mathcal{O}_{a,\sigma} = \{\sigma^n(a) \mid n \in \mathbb{Z}\}$.
- A permutation $\sigma \in S_n$ is called a *cycle* if it has at most one orbit containing more than one element. The *length* of the cycle is the number of elements in that orbit.
- **Theorem:** Every permutation of a finite set can be written as the finite product of disjoint cycles.
- A *transposition* is a cycle of length 2.
- **Theorem:** Every permutation of a finite set is a product of transpositions.
- **Theorem:** Every permutation can be written as either an odd or even number of transpositions.
- The set of partitioned even transpositions is called the *alternating group*.
- A *permutation matrix* is one that has a single 1 per row/col and everything else are 0s. If the determinant of the matrix is 1, then the number of transpositions are even, otherwise, they are odd.

Examples:

1. Find the orbit of 1 under $\sigma = \begin{pmatrix}1&2&3&4&5&6\\3&7&6&7&4&1\end{pmatrix}$: $\sigma^0(1) = 1$, $\sigma^1(1) = 3$, $\sigma^2(1) = \sigma^1(3) = 6$, $\sigma^3(1) = 1$. Thus, the orbit is $\mathcal{O}_{1,\sigma} = \{1, 3, 6\}$.
2. Write $\begin{pmatrix}1&2&3&4&5&6&7&8\\3&8&6&7&4&1&5&2\end{pmatrix}$ as a cycle: $\sigma = (1, 3, 6)(2, 8)(4, 7, 5)$.

2.10 Cosets & Lagrange's Theorem

Definitions:

- Let G be a group with H as a subgroup, and $a \in G$. We define $aH = \{ah \mid h \in H\}$. This is the *left coset* of H. Similarly, $Ha = \{ha \mid h \in H\}$ is a *right coset*. (Generally not a subgroup.)
- Let H be a subgroup of group G. The number of left cosets of H in G is the *index* $(G : H)$ *of H in G*.
- **Lagrange's Theorem:** If G is a finite group with H as a subgroup, then $|H|$ is a divisor of G.
- **Corollary:** If group G has a prime order, the only subgroups are the trivial subgroup and G. Therefore, this group must be cyclic.

Examples:

1. Let $\sigma = (1, 2, 5, 4)(2, 3)$ in S_5. Find the index of $\langle\sigma\rangle$ in S_5. We can rewrite σ as $(1, 2, 3, 5, 4)$ to help with composing. Following that, we get $\sigma^2 = (1, 3, 4, 2, 5)$, $\sigma^3 = (1, 5, 2, 4, 3)$, $\sigma^4 = (1, 4, 5, 3, 2)$, and $\sigma^5 = e$. Therefore, $|\langle\sigma\rangle| = 5$, and the index of $\langle\sigma\rangle$ in S_5 is $|S_5|/|\langle\sigma\rangle| = 120/4 = 30$
2. Let $\mu = (1, 2, 4, 5)(3, 6)$ in S_6. Find the index of $\langle\mu\rangle$ in S_6. Because we are using disjoint cycles, the transposition cycle is the identity element when the power of μ is even. We can make the same connection for the 4-element cycle: when the power of μ is a multiple of 4, it is equal to the identity element. We know that $\mu^4 = e$, $|\langle\mu\rangle| = 4$, and the index of $\langle\mu\rangle$ in S_6 is $720/4 = 180$.
3. Let H be a subgroup of a group G. Prove that if the partition of G into left cosets of H is the same as the partition into right cosets of H, then $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$. *Solution.* The statement "If the partition of G into left cosets of H is the same as the partition into right cosets of H," implies $gH = Hg$ for all $g \in G$. Now, let $g \in G$ and $h \in H$. Our goal is to show that $g^{-1}hg \in H$. Consider the element hg. Since $h \in H$, $hg \in Hg$. Because $Hg = gH$, it must be that $hg \in gH$. By definition of left coset, $hg \in gH$ means that $hg = gh'$ for some $h' \in H$. So, we just solve for this h'. We start by multiplying both sides on the left by g^{-1}: $g^{-1}(hg) = g^{-1}(gh') = (g^{-1}g)h' = h'$. Since $h' \in H$, we have shown that $g^{-1}hg \in H$.
4. Recall the multiplication table for S_3:

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Left coset table:

	ρ_0	μ_3	ρ_1	μ_2	ρ_2	μ_1
ρ_0	ρ_0	μ_3	ρ_1	μ_2	ρ_2	μ_1
μ_3	μ_3	ρ_0	μ_1	ρ_2	μ_2	ρ_1
ρ_1	ρ_1	μ_2	ρ_2	μ_1	ρ_0	μ_3
μ_2	μ_2	ρ_1	μ_3	ρ_0	μ_1	ρ_2
ρ_2	ρ_2	μ_1	ρ_0	μ_3	ρ_1	μ_2
μ_1	μ_1	ρ_2	μ_2	ρ_1	μ_3	ρ_0

2.10 (cont.)

Examples:

4. (a) List the left cosets of the subgroup $\{\rho_0, \mu_3\}$.
   Solution. $\{\rho_0, \mu_3\}$, $\{\rho_1, \mu_2\}$, $\{\rho_2, \mu_1\}$. (This is found by just multiplying $\{\rho_0, \mu_3\}$ by ρs and μs until we get non-unique elements.)
   (b) Does this create a coset group? *Solution.* No. The the table is not made up of the blocks that correspond to the elements defined in (a).

2.11 Direct Products & Finitely Generated Abelian Groups

Definitions:

- The *cartesian product of sets*, $S_1, S_2, \ldots, S_n$ is the set of all n-tuples $a_1, a_2, \ldots, a_n$ where $a_i \in S_i$ for $i = 1, 2, \ldots, n$. The cartesian product is denoted by either $S_1 \times S_2 \times \cdots \times S_n$.
- **Theorem:** If G_1 and G_2 are groups, we define the *direct product* $G_1 \times G_2 = \{(a, b) \mid a \in G_1, b \in G_2\}$ and $G_1 \times G_2$ will have binary operation $(a_1, b_1)(a_2, b_2) = (a_1a_2b_1b_2)$. Also, $\prod_{i=1}^{n} G_i$ is a group, and the direct product of the group G_i under this operation.
- **Theorem:** Let $a_1, a_2, \ldots, a_n \in \prod_{i=1}^{n} G_i$. If each a_i has order r_i in G_i, then the order of $a_1, a_2, \ldots, a_n$ is the *least common multiple* of $r_1, r_2, \ldots, r_n$.
- **Theorem:** Every finitely generated abelian group G is isomorphic to a direct product of the form $\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$, where each p_i is prime, but not necessarily distinct and each r_i are positive integers.
- **Theorem:** $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if m, n are relatively prime. Similarly, $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ if, and only if every pair of m_i and m_j are relatively prime.
- A group G is decomposable if it is isomorphic to a direct product of proper nontrivial subgroups.

Examples:

1. Find the order of $(8, 4, 10)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$. 8 in $\mathbb{Z}_{12}$ is $\frac{12}{\gcd(8,12)} = 3$. 4 in $\mathbb{Z}_{60}$ is $\frac{60}{\gcd(4,60)} = 15$. 10 in $\mathbb{Z}_{24}$ is $\frac{24}{\gcd(10,24)} = 12$. The order is $\operatorname{lcm}(3, 15, 12) = 60$.
2. Consider this permutation from S_9 : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 9 & 2 & 7 & 5 & 1 & 3 & 8 \end{pmatrix}$.
   (a) Express σ as a product of disjoint cycles. (b) What is the order of σ? (c) Express σ as a product of transpositions. (d) Is σ an even or odd permutation? *Solutions.* (a) $(1, 6, 5, 7)(2, 4)(3, 9, 8)$. (b) Notice $(1, 6, 5, 7)$ has order 4, and the others have order 2 and 3 respectively. Thus, the order is $\operatorname{lcm}(4, 2, 3) = 12$. (c) $(1, 6)(6, 5)(5, 7)(2, 4)(3, 9)(9, 8)$. (d) even.
3. Consider the group $\mathbb{Z}_{12} \times \mathbb{Z}_8 \times \mathbb{Z}_{15}$. Is this group isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_{45} \times \mathbb{Z}_8$? *Solution.* No. $\mathbb{Z}_{45} \simeq \mathbb{Z}_9 \times \mathbb{Z}_5 \not\simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ because of prime relativity.
4. Find all abelian groups, up to isomorphism, of order 360. *Solution.* This can be factored into $2^3 3^2 5$. We get 6 abelian groups of order 360:
   (1) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
   (2) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
   (3) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
   (4) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
   (5) $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
   (6) $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

3.13 Homomorphisms

Definitions:

For these definitions, φ is a homomorphism from G to G', unless stated otherwise.

- A map φ of a group G into a group G' is a *homomorphism* if the homomorphism property $\varphi(a * b) = \varphi(a) *' \varphi(b)$ holds for all $a, b \in G$. The *trivial homomorphism* is $\varphi : G \to G'$, $\varphi(g) = e'$.
- **Theorem:** Let G, G' be groups with φ. Then φ has the following properties:
  1. $\varphi(e) = e'$. 2. If $a \in G$, then $\varphi(a^{-1}) = \varphi(a)^{-1}$.
  3. If H is a subgroup of G, then $\varphi[H]$ is a subgroup of G'.
  4. If K' is a subgroup of G', then $\varphi^{-1}[K']$ is a subgroup of G.
- Let φ be a mapping of a set X into a set Y, and let $A \subseteq X$ and $B \subseteq Y$. The *image $\varphi[A]$ of A in Y under φ* is $\{\varphi(a) \mid a \in A\}$. The set $\varphi[X]$ is the *range of φ*. The *inverse image $\varphi^{-1}[B]$ of B in X* is $\{x \in X \mid \varphi(x) \in B\}$
- The subgroup $\varphi^{-1}[\{e'\}] = \{x \in G \mid \varphi(x) = e'\}$ is called the *kernel* of φ. $\ker(\varphi)$ is a subgroup of G.
- **Theorem:** Let $\varphi : G \to G'$, $H = \ker(\varphi)$, and $a \in G$. Then $aH = \{x \in G \mid \varphi(x) = \varphi(a)\} = Ha$.
- φ is 1-1 iff $\ker(\varphi) = \{e\}$. (φ has a trivial kernel.)
- A subgroup H of G is called a *normal subgroup* if for all $g \in G$, $gH = Hg$. Every subgroup of an abelian subgroup is normal. Equivalent definitions:
  – $\forall g \in G,\ h \in H,\ ghg^{-1} \in H$. – $\forall g \in G, gHg^{-1} = H$.

Examples:

1. Let $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_2$ be given by $\varphi(x) =$ the remainder of x when divided by 2, as in the division algorithm. Determine if φ is a homomorphism. *Solution.* We know $\varphi(x) = x \bmod 2$, and we have binary operators $(a+b) \bmod 6$ for $\mathbb{Z}_6$ and $(a + b) \bmod 2$ for $\mathbb{Z}_2$. This leaves us with the following equation to check: $\varphi((a + b) \bmod 6) = (\varphi(a) + \varphi(b)) \bmod 2$. For the left-hand side: $\varphi((a + b) \bmod 6) = ((a + b) \bmod 6) \bmod 2$. This simplifies down to $(a + b) \bmod 2$ since $6 \equiv 0 \pmod 2$. For the right-hand side: $(\varphi(a)+\varphi(b)) \bmod 2 = (a \bmod 2 + b \bmod 2) \bmod 2$. Since addition is commutative and associative in both groups, we can rewrite this as: $(a+b) \bmod 2$. Therefore, the equation holds, and the map is a homomorphism.
2. Let $\varphi : \mathbb{Z}_9 \to \mathbb{Z}_2$ be given by $\varphi(x) =$ the remainder of x when divided by 2, as in the division algorithm. *Solution.* This is not a homomorphism because the two sides of the equation are not equal: $\varphi((3 + 7) \bmod 9) = \varphi(1) = 1 \neq (\varphi(3) + \varphi(7)) \bmod 2 = (1 + 1) \bmod 2 = 0$.
3. Compute $\ker(\varphi)$ and $\varphi(20)$ for $\varphi : \mathbb{Z} \to S_8$ such that $\varphi(1) = (1, 4, 2, 6)(2, 5, 7)$. *Solution.* We know $\varphi(1) = (1, 4, 2, 6)(2, 5, 7) = (1, 4, 2, 5, 7, 6)$ has order 6, so $\ker(\varphi) = 6\mathbb{Z}$. Then, we know from the homomorphism property that $\varphi(20) = (\varphi(1))^{20} = (\varphi(1))^{18}(\varphi(1))^2 = (\varphi(1))^2 = (1, 2, 7)(4, 5, 6)$.

3.14 Factor Groups

Definitions:

For these definitions, φ is a homomorphism from G to G', unless stated otherwise.

- **Fundamental Theorem of Homomorphisms:** Let $\varphi : G \to G'$ with $H = \ker(\varphi)$. Then the cosets of H form a *factor group*, G/H, where $(aH)(bH) = (ab)H$. Also, the map $\mu : G/H \to \varphi[G]$ defined by $\mu(aH) = \varphi(a)$ is an isomorphism. both coset multiplication and μ are well defined, independent of the choices a and b from the cosets.
- **Theorem:** Let $H \leq G$. Coset multiplication is well defined iff H is a normal subgroup of G.
- **Theorem:** Let H be a normal subgroup of G. Define $\gamma : G \to G/H$ by $\gamma(g) = gH$. Then γ is a homomorphism with kernel H.
- An isomorphism $\varphi : G \to G$ is called an *automorphism.*
- For a given $g \in G$, the map $i_g : G \to G$ defined by $i_g(x) = gxg^{-1}$ is called the *inner automorphism* of G by g, and $i_g(x)$ is the *conjugation of x by g.*
- For a subgroup H of G, $i_g[H] = \{ghg^{-1} \mid h \in H\}$ is called a *conjugate subgroup* of H.

Examples:

1. Find the order of $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/(\langle 2\rangle \times \langle 2\rangle)$. *Solution.* In $\mathbb{Z}_4$, the subgroup generated by $\langle 2\rangle$ is $\{0, 2\}$. Then, in $\mathbb{Z}_{12}$, the subgroup generated by $\langle 2\rangle$ is $\{0, 2, 4, 6, 8, 10\}$. Thus, the subgroup $\langle 2\rangle \times \langle 2\rangle$ has order $2 \times 6 = 12$, and $\mathbb{Z}_4 \times \mathbb{Z}_{12}$ has order $4 \times 12 = 48$. By Lagrange's Theorem, the order of the factor group is $48/12 = 4$.
2. Find the order of $(\mathbb{Z}_{12} \times \mathbb{Z}_{18})/\langle(4, 3)\rangle$. *Solution.* The order of $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$ is $12 \times 18 = 216$. In $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$, the subgroup generated by $\langle(4, 3)\rangle$ has order 6. So, by Lagrange's Theorem, the order of the factor group is $216/6 = 36$.
3. Find the order of the element in the factor group:
   (a) $(2, 1) + \langle(1, 1)\rangle$ in $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle(1, 1)\rangle$. *Solution.* In $\mathbb{Z}_3 \times \mathbb{Z}_6$, $\langle(1, 1)\rangle = \{(1, 1), (2, 2), (0, 3), (1, 4), (2, 5), (0, 0)\}$. Then, we test the powers of $(2, 1)$ until we find one that is in $\langle(1, 1)\rangle$: $(2, 1)(2, 1) = (1, 2) \implies (1, 2)(2, 1) = (0, 3)$. So, the order of $(2, 1) + \langle(1, 1)\rangle$ in $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle(1, 1)\rangle$ is 3.

3.15 Factor Group Computations

Definitions:

- A group is called *simple* if it is nontrivial and has no proper nontrivial normal subgroups (i.e., only the identity and the group itself.)
- A *maximal normal subgroup* of a group G is a normal proper subgroup M for which there is no normal proper subgroup of G which properly contains M.
- **Theorem:** M is a maximal normal subgroup of G iff G/M is simple.
- **Theorem:** Let $\varphi : G \to G'$ be a group homomorphism. If N is a normal subgroup of G, then $\varphi[N]$ is a normal subgroup of $\varphi[G]$. If N' is a normal subgroup of $\varphi[G]$, then $\varphi^{-1}[N']$ is a normal subgroup of G.
- We define the *center of a group* to be $Z(G) = \{z \in G \mid \forall g \in G, zg = gz\}$. $Z(G)$ is a normal subgroup.
- For any $a, b \in G$, consider $aba^{-1}b^{-1}$. If a and b commute, then $aba^{-1}b^{-1} = e$, if they don't then $aba^{-1}b^{-1}$ is not the identity. Each $aba^{-1}b^{-1}$ is called a *commuter* of G. The *commutator subgroup* of G is the subgroup generated by the commutators. This is the set of finite products of commutators, which is not abelian.

Examples: (For 1-4, classify the group according to the fundamental theorem of finitely generated abelian groups)

1. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(0, 1)\rangle$. *Solution.* $\langle(0, 1)\rangle$ has order 4, so $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(0, 1)\rangle$ has order 2. Therefore, this leaves only one choice: $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(0, 1)\rangle \simeq \mathbb{Z}_2$.
2. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(1, 2)\rangle$. *Solution.* $\langle(1, 2)\rangle$ has order 2, so $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(1, 2)\rangle$ has order 4. This leaves us with two choices: $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Since $(1, 1) + \langle(1, 2)\rangle$ has order 4 in the factor group, we must have $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(1, 2)\rangle \simeq \mathbb{Z}_4$.
3. $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1, 2)\rangle$. *Solution.* $|\langle(1, 2)\rangle| = 4 \implies |(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1, 2)\rangle| = 8$. Therefore, either $\mathbb{Z}_8$ or $\mathbb{Z}_4 \times \mathbb{Z}_2$. Since $|(0, 1) + \langle(1, 2)\rangle| = 8$, $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1, 2)\rangle \simeq \mathbb{Z}_8$.
4. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/\langle(1, 1, 1)\rangle$. *Solution.* The 1 in the generator $(1, 1, 1)$ of $\langle(1, 1, 1)\rangle$ shows that each coset of $\langle(1, 1, 1)\rangle$ contains a unique element of the form $(0, m, n)$, and of course, every such element of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is in some coset of $\langle(1, 1, 1)\rangle$. We can choose these representatives $(0, m, n)$ to compute in the factor group, which therefore must be isomorphic to $\mathbb{Z} \times \mathbb{Z}$.
5. Find both the center and the commutator subgroups of $\mathbb{Z}_3 \times S_3$. *Solution.* Because ρ_0 is the only element of S_3 that commutes with every element of S_3, we see that $Z(\mathbb{Z}_3 \times S_3) = \mathbb{Z}_3 \times \{\rho_0\}$. Because A_3 is in the commutator subgroup of S_3, we see that the commutator subgroup of $\mathbb{Z}_3 \times S_3$ is $\{0\} \times S_3$.