Algebra Exam 2 Note Sheets

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.)
- **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 (from Example 9.14). 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. Thus, 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}:

$$\begin{aligned} g^{-1}(hg) &= g^{-1}(gh') \\ g^{-1}hg &= (g^{-1}g)h' \\ g^{-1}hg &= h'. \end{aligned}$$

Since $h' \in H$, we have shown that $g^{-1}hg \in H$.

2.10 (cont.)

Examples:

4. Let S_A be the group of all permutations of the set A, and let c be one particular element of A. Show that $\{\sigma \in S_A \mid \sigma(c) = c\}$ is a subgroup $S_{c,c}$ of S_A. *Solution.* **Identity:** The identity permutation e maps every element to itself, so $e(c) = c$. Thus, $e \in S_{c,c}$. **Closure:** Let $\sigma, \tau \in S_{c,c}$. This means $\sigma(c) = c$ and $\tau(c) = c$. We must check their product: $(\sigma\tau)(c) = \sigma(\tau(c)) = \sigma(c) = c$. **Inverses:** Let $\sigma \in S_{c,c}$. As before, this means $\sigma(c) = c$, and we also have to check σ^{-1}. We will do this by multiplying σ^{-1} to both sides of the equation:

$$\sigma^{-1}(\sigma(c)) = \sigma^{-1}(c) \implies (\sigma^{-1}\sigma)(c) = \sigma^{-1}(c) \implies e(c) = \sigma^{-1}(c)$$

Because $\sigma^{-1}(c) = c$, the inverse σ^{-1} is in $S_{c,c}$. Since $S_{c,c}$ contains the identity, is closed under the binary operation, and is closed under inverses, it is a subgroup of S_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:** $\mathbb{Z}_n \times \mathbb{Z}_n$ 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 $\operatorname{lcm}(3, 15, 12) = 60$.

Extra Problems

Examples:

8:47 For S_n, show that if $n \geq 3$, then the only element of σ of S_n satisfying $\sigma\gamma = \gamma\sigma$ for all $\gamma \in S_n$ is $\sigma = i$, the identity permutation. *Solution.* Suppose $\sigma(i) = m \neq i$. Define $\gamma \in S_n$ such that $\gamma(i) = i$ and $\gamma(m) = r$ where $r \neq m$. (Note this is possible because $n \geq 3$.) Then $\sigma\gamma(i) = \sigma(\gamma(i)) = \sigma(i) = m$ while $\gamma\sigma = \gamma(\sigma(i)) = \gamma(m) = r$, so $\sigma\gamma \neq \gamma\sigma$. Thus $\sigma\gamma = \gamma\sigma$ for all $\gamma \in S_n$ only if σ is the identity permutation.

9:31 Let A be an infinite set. Let H be the set of all $\sigma \in S_A$ such that the number of elements moved by σ ("σ **moves** $a \in A$" if $\sigma(a) \neq a$) is finite. Show that H is a subgroup of S_n. *Solution.* **Closure:** Let $\sigma, \mu \in H$. If σ moves elements $s_1, s_2, \ldots, s_k$ of A, and μ moves elements $r_1, r_2, \ldots, r_m$ of A, then $\sigma\mu$ can't move any elements not in the list $s_1, s_2, \ldots, s_k, r_1, r_2, \ldots, r_m$, so $\sigma\mu$ moves at most a finite number of elements of A, and hence in H. Thus, H is closed under the operation of S_A. **Identity:** The identity permutation is in H because it moves no elements of A. **Inverses:** Because the elements moved by $\sigma \in H$ are the same as the elements moved by σ^{-1}, we see that for each $\sigma \in H$, we have $\sigma^{-1} \in H$ also. Thus, H is a subgroup of S_A.

X:34 Let G be a group of order pq, where p and q are prime numbers. Show that every proper subgroup of G is cyclic. *Solution.* The possible orders for a proper subgroup are p, q and 1. Now p and q are primes and every group of prime order is cyclic, and of course every group of order 1 is cyclic. Thus, every proper subgroup of a group of order pq must be cyclic.

X:36 A previous problem showed that every finite group of even order $2n$ contains an element of order 2. Using Lagrange's theorem, show that if n is odd, then an abelian group of order $2n$ contains precisely one element of order 2. *Solution.* Let G be abelian of order $2n$ where n is odd. Suppose that G contains two elements, a and b, of order 2. Then $(ab)^2 = abab = aabb = ee = e$ and $ab \neq e$ because the inverse of a is a itself. Thus ab also has order 2. It is easily checked that then $\{e, a, b, ab\}$ is a subgroup of G of order 4. But this is impossible because n is odd and 4 does not divide $2n$. Thus, there can't be two elements of order 2.

X:37 Show that a group with at least two elements but with no proper nontrivial subgroups must be finite and of prime order. *Solution.* Let G be of order ≥ 2 but with no proper nontrivial subgroups. Let $a \in G$, $a \neq e$. Then $\langle a \rangle$ is a nontrivial subgroup of G, and thus must be G itself. Because every cyclic group not of prime order has proper subgroups, we see that G must be finite of prime order.

11:16 Are the groups $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $\mathbb{Z}_4 \times \mathbb{Z}_6$ isomorphic? Why or why not? *Solution.* When we split these into two separate decompositions, we will see that they are isomorphic. First, we know that $\mathbb{Z}_{mn} \simeq \mathbb{Z}_n \times \mathbb{Z}_m \iff \gcd(n,m) = 1$. Since 12 is not a prime number and $\gcd(3,4) = 1$, then $\mathbb{Z}_{12} \simeq \mathbb{Z}_3 \times \mathbb{Z}_4$, and $\mathbb{Z}_2 \times \mathbb{Z}_{12} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$. The same thing applies for $\mathbb{Z}_6$. It decomposes into $\mathbb{Z}_2 \times \mathbb{Z}_3$ because $\gcd(2,3) = 1$. Thus, $\mathbb{Z}_4 \times \mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$. Since both $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $\mathbb{Z}_4 \times \mathbb{Z}_6$ decompose into the same product, they are isomorphic.