A First Course in Abstract Algebra by Fraleigh 7th Edition (Notes Part II)

Hubert Farnsworth

July 8, 2018

1 Part II : Permutations, Cosets, and Direct Products

1.1 Groups of Permutation

8.3 Definition A **permutation of a set** A is a bijective function $\phi : A \to A$.

8.5 Theorem Let A be a nonempty set and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.

8.6 Definition Let A be the finite set $\{1, 2, ..., n\}$. The group of all permutations of A is the **symmetric group on n letters**, and is denoted S_n.

8.14 Definition Let $f : A \to B$ be a function and let $H \subseteq A$. The **image of H under f** is $\{f(h) \mid h \in H\}$ and is denoted $f[H]$.

8.15 Lemma Let G and G' be groups and let $\phi : G \to G'$ be an injective homomorphism. Then $\phi[G] \leq G'$ and ϕ provides an isomorphism of G with $\phi[G]$.

8.16 Theorem (Cayley's Theorem) Every group is isomorphic to a group of permutations.

8.17 Definition The map $\phi : G \to S_G,\ \phi(x) = \lambda_x$, where $\lambda_x : G \to G,\ \lambda_x(g) = xg\ \forall g \in G$ (in the proof of Theorem 8.16) is the **left regular representation of G**, and the map $\mu : G \to S_G,\ \mu(x) = \rho_{x^{-1}}$ is the **right regular representation of G**

Notable Exercises

Let A be a set and let $\sigma \in S_A$. For a fixed $a \in A$, the set

$$\mathscr{O}_{a,\sigma} = \{\sigma^n(a) \mid n \in \mathbb{Z}\}$$

is the **orbit of a under σ**

11) Find $\mathscr{O}_{1,\sigma}$ where $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$.

(Answer) : We have, under the mapping σ, $1 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 6 \mapsto 2 \mapsto 1$. Therefore, $\mathscr{O}_{1,\sigma} = \{1, 2, 3, 4, 5, 6\}$.

17) Find the number of elements in the set $\{\sigma \in S_5 \mid \sigma(2) = 5\}$.

(Answer) : This is a combinatorial problem - how many ways can we order the elements of the set $\{1, 2, 3, 4, 5\}$ such that we have 2 as the last position of the ordering? With one position fixed, there remain $4! = 24$ ways to arrange the remaining numbers.

35) Mark the following statements as true or false :

(Answers) :

a. Every permutation is a one to one function. – True (by definition a permutation must be a one to one function among other characteristics).

c. Every function from a finite set onto itself must be one to one. – True. Suppose A is a set. If $A = \emptyset$, this statement holds vacuously, so suppose $|A| = n \in \mathbb{N}$. Let $\phi : A \to A$ be an onto function. Suppose ϕ is not one to one. Then $\phi(a) = \phi(b) = c \in A$ for some $a, b \in A$ $a \neq b$. Then we must map the remaining $n - 2$ elements of A that are neither a, b to the $n - 1$ elements of A that are not c in order to satisfy the assumption that ϕ is onto. Since ϕ is a function, we may map each of these $n - 2$ elements to at most one of the $n - 1$ elements in the image. We cannot map $n - 2$ elements to $n - 1$ elements, so that ϕ cannot be an onto function. This is a contradiction, so we conclude ϕ must be one to one.

e. Every subgroup of an abelian group is abelian. – True. Let G be an abelian group and let $H \leq G$ and suppose H is not abelian. Then there exist $a, b \in H$ such that $ab \neq ba$. But then since $H \subseteq G$, this shows that $a, b \in G$ and $ab \neq ba$, so that G is not an abelian group. This is a contradiction, so we must conclude that if G is abelian, any subgroup of G must also be abelian.

g. The set S_10 has 10 elements. – False. $|S_10| = 10!$ since there are 10! permutations of 10 distinct objects.

i. S_n is not cyclic for any n. – False. Consider S_1, the set of all permutations of $\{1\}$. The identity permutation of this set is the only element of S_1, and thus $\langle i \rangle = S_1$, meaning S_1 is cyclic.

1.2 Orbits, Cycles, and the Alternating Groups

For $a, b \in A$, let $a \sim b$ iff $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$. It is somewhat straightforward to verify that $\sim$ defines an equivalence relation on A.

9.1 Definition Let σ be a permutation of the set A. The equivalence classes in A determined by $\sim$ above are called the **orbits of** σ.

9.6 Definition A permutation $\sigma \in S_n$ is a **cycle** if it has at most one orbit containing more than one element. The **length** of a cycle is the number of elements in its largest orbit.

9.8 Theorem Every permutation σ of a finite set is a product of disjoint cycles.

9.15 Theorem No permutation in S_n can be written as the product of an even number of transpositions and as an odd number of transpositions.

9.20 Theorem If $n \geq 2$, then the collection of all even permutations of $\{1, 2, ..., n\}$ forms a subgroup of order $n!/2$ of the symmetric group S_n.

9.21 Definition The subgroup of S_n consisting of the even permutations of n letters is the **alternating group A_n on n letters**.

Notable Exercises

1) Find all orbits of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 6 & 2 & 4 \end{pmatrix}$.

(Answer) : $1 \mapsto 5 \mapsto 2 \mapsto 1$, $3 \mapsto 3$, $4 \mapsto 6 \mapsto 4$. So the orbits of this permutation are :

$$\{1, 2, 5\},\ \{3\},\ \{4, 6\}\ .$$

5) Find all orbits of the permutation $\sigma : \mathbb{Z} \to \mathbb{Z}$, $\sigma(n) = n + 2$.

(Answer) : Going back to the definition, and letting $k\mathbb{Z}$ be arbitrary, we have $\mathscr{O}_{k,\sigma} = \{\sigma^p(k) \mid p \in \mathbb{Z}\} = \{k + 2p \mid p \in \mathbb{Z}\}$. From this it is more clear that we have two possible orbits depending on whether k is even or odd since if k is even, $k + 2p$ is even for all p and similarly if k is odd, $k + 2p$ is odd for all p. So we conclude that the orbits of σ are :

$$\{2j \mid j \in \mathbb{Z}\},\ \{2j + 1 \mid j \in \mathbb{Z}\}\ .$$

7) Compute the permutation $(1, 4, 5)(7, 8)(2, 5, 7)$ of $\{1, 2, 3, 4, 5, 6, 7, 8\}$.

A nice way of doing these types of problems without too much writing/computating is as follows : With each number in order, work through the cycles from right to left looking for the first appearance (if no appearances then this number is unchanged) and then following what this number maps to as you continue working left. Some examples will make this more clear.

$1 \mapsto 4$, $2 \mapsto 5 \mapsto 1$, 3 unchanged, $4 \mapsto 5$, $5 \mapsto 7 \mapsto 8$, 6 unchanged, $7 \mapsto 2$, $8 \mapsto 7$. So our result is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 3 & 5 & 8 & 6 & 2 & 7 \end{pmatrix}\ .$$

19) In drawing the Cayley digraph, it is helpful to remember that when direction matters, moving in the direction of the arrow means applying the permutation $(1, 2, 3)$ on the right of the element at the current node.

23) Mark the following as true or false.

a. Every permutation is a cycle. – False. A cycle is a permutation that has at most one orbit with more than one element. See exercises 1,5 above for permutations that are not cycles.

e. A_5 has 120 elements. – False. $|A_5| = 5!/2 = 60 \neq 120$.

A_3 is a commutative group. – True. We know that A_3 is a group by Theorem 9.20 with $3!/2 = 3$ elements. We have established that any group with 3 elements is abelian. We could also manually find the 3 elements of A_3 and check this, but using theorems is faster.

i. S_7 is isomorphic to the subgroup of all those elements of S_8 that leave the number 5 fixed. – True. Call the subgroup of all those elements of S_8 that leave the number 5 fixed H. Then $|H| = 7! = |S_7|$. Define $\phi : H \rightarrow S_7$ such that for any $\sigma \in H$, ϕ maps σ to the permutation $\mu \in S_7$ for which $\mu(1) = \sigma(1), \mu(2) = \sigma(2), ..., \mu(4) = \sigma(4), \mu(5) = \sigma(6), \mu(6) = \sigma(7), \mu(7) = \sigma(8)$. We know this is possible since σ is a permutation of the elements of the set $\{1, 2, 3, 4, 6, 7, 8\}$, which has 7 elements and S_7 is the set of all permutations of the elements of the set $\{1, 2, 3, 4, 5, 6, 7\}$ and the fact that the naming of the elements of these sets is slightly different does not matter since they have the same number of elements.

1.3 Cosets and the Theorem of Lagrange

10.1 Theorem Let $H \leq G$. Let the relation $\sim_L$ be defined on G by

$$a \sim_L b \text{ iff } a^{-1}b \in H.$$

Let $\sim_R$ be defined by

$$a \sim_R b \text{ iff } ab^{-1} \in H.$$

Then $\sim_L$ and $\sim_R$ are both equivalence relations on G.

Discussion : What is the set of all $x \in G$ such that $a \sim_L x$? Well this is the set of $x \in G$ such that $a^{-1}x \in H$, or in other words $a^{-1}x = h$ for some $h \in H$. Equivalently, this means $x = ah$. So the cell in the partition of G made by the equivalence relations $\sim_L$ is $\{ah \mid h \in H\}$. We denote this set $aH = \{ah \mid h \in H\}$. Similarly we may define $Ha = \{ha \mid h \in H\}$.

10.2 Definition Let H be a subgroup of group G. The subset aH of G is the **left coset** of H containing a, while the subset Ha is the **right coset** of H containing a.

Note : Every coset of a subgroup H of group G has the same number of elements as H. The text proves this rigorously by defining a bijective function between H and an arbitrary left coset gH (and the logic can be recycled to show the result for a right coset). My intuition is this : given H, a coset, WLOG a left coset, is computed (in theory) by taking an element of G and performing ah for every $h \in H$. Clearly we cannot have more ah terms than $h's$ so the coset cannot be larger than H and if the coset has fewer elements than H, that must mean that at least two of the multiplications had the same result, for example $ah_1 = ah_2$ for $h_1 \neq h_2$. But since $a \in G$ and G is a group, we can cancel a, meaning $h_1 = h_2$ after all! I imagine, for the finite case the sets $H = \{h_1, h_2, h_3, ..., h_n\}$ and $aH = \{ah_1, ah_2, ..., ah_n\}$. We have n 'multiplications' and if any two terms collapsed into one it would contradict the assumption that G is a group.

10.10 Theorem (Lagrange) Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

10.11 Corollary Every group of prime order is cyclic.

10.12 Theorem The order of an element of a finite group divides the order of the group.

10.13 Definition Let $H \leq G$. The number of left cosets of H in G is the **index** $(G : H)$ **of** H **in** G.

10.14 Theorem Suppose $K \leq H \leq G$, and suppose both $(G : H)$ and $(H : K)$ are finite. Then $(G : K)$ is finite and $(G : K) = (G : H)(H : K)$.

Notable Exercises

5) Find all the cosets of the subgroup $\langle 18 \rangle$ of $\mathbb{Z}_{36}$.

(Answer) : First note that $\mathbb{Z}_{36}$ is abelian so in finding all the left cosets we automatically have found all the right cosets (and vice versa of course). We just start finding left cosets :

$$\langle 18 \rangle = \{18, 0\}$$

$$1 + \langle 18 \rangle = \{19, 1\}$$

$$2 + \langle 18 \rangle = \{20, 2\}$$

$$....$$

$$17 + \langle 18 \rangle = \{35, 17\}\ .$$

Notice that $18 + \langle 18 \rangle = \langle 18 \rangle$, $19 + \langle 18 \rangle = 1 + \langle 18 \rangle$,...$35 + \langle 18 \rangle = 17 + \langle 18 \rangle$, so that we get no new distinct cosets beyond the 18 cosets described above. That means the cosets given above are all the left cosets (= right cosets).

15) Let $\sigma = (1, 2, 5, 4)(2, 3) \in S_5$ (recall S_5 is the set of all permutations of the elements of the set $\{1, 2, 3, 4, 5\}$). Find the index of $\langle \sigma \rangle$ in S_5.

(Answer) : First we know $\sigma^0 = i$, where $i \in S_5$ is meant here to be the identity permutation and also we are given σ by the question itself. My approach is to just start find σ^n for larger positive exponents (we get negative exponents by just reversing changes made by a positive exponent permutation, but we won't need to list them to get the answer). We find, using techniques described in the previous section, that :

$$\sigma^2 = (1, 3, 4, 2, 5),\ \sigma^3 = (1, 5, 2, 4, 3),\ \sigma^4 = (1, 4, 5, 3, 2),\ \sigma^5 = i\ .$$

Therefore, $|\langle \sigma \rangle| = |\{i, \sigma, \sigma^2, \sigma^3, \sigma^4\}| = 5$. Since $|S_5| = 5! = 120$, and since the order of every coset must be the same as the order of the 'identity' coset we just found, we conclude that $(S_5 : \langle \sigma \rangle) = 120/5 = 24$.

19) Mark the following statements as true or false.

c. Every group of prime order is abelian. – True. Every group of prime order is cyclic by corollary 10.11 and every cyclic group is abelian by a previous theorem (if G is cyclic with generator g, then for $a, b \in G$, we have $a = g^m, b = g^n$ for some $m, n \in \mathbb{Z}$, so that $ab = g^m g^n = g^{m+n} = g^n g^m = ba$).

e. A subgroup of a group is a left coset of itself. – True. We interpret this to mean if $H \leq G$, H is a left coset of H, which is true, since we just take $e \in G$ and form the left coset $eH = \{eh \mid h \in H\} = H$. In fact we have used this without proof quite a bit in the exercises since it seemed clear, but it does not hurt to give some justification.

g. A_n is of index 2 in S_n for $n > 1$. – True. Suppose $S_n = \{\sigma_0 = i, \sigma_1, \sigma_2, ..., \sigma_{n!}\}$. Let $\sigma_k \in S_n$, and consider, (wlog) the left coset $\sigma_k A_n$. If σ_k is an even permutation, then since A_n is the group of even permutations (and therefore closed), $\sigma_k A_n = A_n$. If σ_k is not an even permutation, σ_k must be an odd permutation and since the composition of an odd permutation with an even permutation is odd, $\sigma_k A_n$ is the set of all odd permutations in S_n. These are the only two possibilities since a permutation must be either even or odd. Therefore $(S_n : A_n) = 2$.

i. Every finite group contains an element of every order that divides the order of the group. – False. The meaning is hard to understand, but it appears to be the converse of Theorem 10.10, which is not necessarily true unless the group is abelian. See the discussion following Theorem 10.14.

1.4 Direct Products and Finitely Generated Abelian Groups

11.2 Theorem Let $G_1, ..., G_n$ be groups. For $(a_1, ..., a_n), (b_1, ..., b_n) \in \prod_{i=1}^n G_i$, define $(a_1, ..., a_n)(b_1, ..., b_n) = (a_1 b_1, ..., a_n b_n)$ using for each component of the product the operation defined on the group that the component belongs to. Then $\prod_{i=1}^n G_i$ is a group, the **direct product of the groups** G_i, under this binary operation.

Note : If each G_i is commutative, we might see this referred to as the **direct sum of the groups** G_i and use the additive notation instead, $\oplus_{i=1}^n G_i$.

11.5 Theorem The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and isomorphic to the group $\mathbb{Z}_{mn}$ if and only if m, n are relatively prime.

11.8 Definition Let $r_1, r_2, ..., r_n$ be positive integers. Their **least common multiple (lcm)** is the positive generator of the cyclic group of all common multiples of the r_i, that is, the cyclic group of all integers divisible by each r_i, $i = 1, 2, ..., n$.

11.9 Theorem Let $(a_1, ..., a_n) \in \prod_{i=1}^n G_i$. If a_i is of finite order r_i (for each i), then the order of $(a_1, ..., a_n) \in \prod_{i=1}^n G_i$ is equal to the least common multiple of all the r_i.

11.14 Definition A group G is **decomposable** if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is **indecompos-**

able.

11.15 Theorem The finite indecomposable groups are exactly the cyclic groups with order a power of a prime.

11.16 Theorem If m divides the order of a finite abelian group G, then G has a subgroup of order m.

Notable Exercises

1) List the elements of $\mathbb{Z}_2 \times \mathbb{Z}_4$. Find the order of each element. Is this group cyclic.

(Answer) : $\mathbb{Z}_2 \times \mathbb{Z}_4 = \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3)\}$. The orders of the elements are 1,4,2,4,2,4,2,4 respectively. This is found by just adding each element to itself until the identity element, $(0,0)$, results. This group cannot be cyclic since if $\langle g \rangle = \mathbb{Z}_2 \times \mathbb{Z}_4$ for some element g in the group, then the order of g would be 8 (there are 8 elements in the group). This is not the case for any of the elements, as we have seen.

7) Find the order of the element $(3,6,12,16)$ in the group $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20} \times \mathbb{Z}_{24}$.

(Answer) : 3 is of order 4 in $\mathbb{Z}_4$, 6 is of order 2 in $\mathbb{Z}_{12}$, 12 is of order 5 in $\mathbb{Z}_{20}$, and 16 is of order 3 in $\mathbb{Z}_{24}$. The order of $(3,6,12,16)$ will be the least common multiple of the orders of the components in their component groups. We have $lcm(4,2,5,3) = 60$, so $(3,6,12,16)$ is of order 60 in $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20} \times \mathbb{Z}_{24}$.

19) Find the maximum possible order for some element of $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15}$.

(Answer) : The maximum possible order of an element of $\mathbb{Z}_4$ is 4,the maximum possible order of an element of $\mathbb{Z}_{18}$ is 18, and the maximum possible order of an element of $\mathbb{Z}_{15}$ is 15. If all three of these cases occur for some element of $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15}$, then the order of that element is $lcm(4,18,15) = 180$. So this is the maximum possible order of an element of $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15}$ (Since if the order of any of the three components of an element of this group is less than the maximum order of the component group, the order of that element in the direct product groups will be less than 180).

21) Find all abelian groups, up to isormorphism, of order 8.

(Answer) : We have the prime factorization of 8 as $8 = 2^3$, so using the example from the chapter we suggest the groups (ignoring order of the factors in direct products) :

$$\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2\,.$$

41) Let G be an abelian group. The elements of finite order in G form a subgroup, which is called the **torsion subgroup of** G. Find the torsion subgroup of $\langle R^*, \cdot\rangle$.

(Answer) : The identity element of the multiplicative group of nonzero real numbers is 1. The only elements of the set $\{g \in \langle \mathbb{R}^*, \cdot\rangle\ |g^n = 1 \text{ for some } n \in \mathbb{Z}\} \subset \mathbb{R}^*$ are 1 and -1. So the torsion subgroup of $\langle \mathbb{R}^*, \cdot\rangle$ is just $\{-1, 1\}$.

1.5 Plane Isometries

Definition An **isometry of** $\mathbb{R}^2$ is a distance preserving permutation $\phi : \mathbb{R}^2 \to \mathbb{R}^2$, meaning the distance between $\phi(P)$ and $\phi(Q)$ is equal to the distance between P and Q for all $P, Q \in \mathbb{R}^2$ (the author refers to $\mathbb{R}^2$ as the Eudlidean plane, so we are probably using the Euclidean distance function in the plane).

Using function composition as the prevailing binary operation, we can see that the set of isometries of $\mathbb{R}^2$ forms a subgroup of the group of permutations of $\mathbb{R}^2$. Notably the closure property holds by the following : If ψ and ϕ are two isometries of $\mathbb{R}^2$, then the distance between $\psi(\phi(P))$ and $\psi(\phi(Q))$ is equal to the distance between $\phi(P)$ and $\phi(Q)$ which is in turn equal to the distance between P and Q, so that the composition $\psi \circ \phi : \mathbb{R}^2 \to \mathbb{R}^2$ is an isometry of $\mathbb{R}^2$ as well.

Definition Given $S \subset \mathbb{R}^2$, the set of isometries of $\mathbb{R}^2$ that carry S onto S forms a subgroup of the group of isometries of $\mathbb{R}^2$. This subgroup is the **group of symmetries of** S **in** $\mathbb{R}^2$.

12.5 Theorem Every finite group G of isometries of the plane is isomorphic to either $\mathbb{Z}_n$ or to a dihedral group D_n for some $n \in \mathbb{N}$.

Notable Exercises

1)

a. Describe all symmetries of a point in the real line $\mathbb{R}$; that is, describe all isometries of $\mathbb{R}$ that leave one point fixed.

b. Describe all symmetries of a point in the plane $\mathbb{R}^2$.

c. Describe all symmetries of a line segment in $\mathbb{R}$.

d. Describe all symmetries of a line segment in $\mathbb{R}^2$.

(Answers) :

a. Given a point c, define an isometry $\phi : \mathbb{R} \to \mathbb{R}$ by $\phi(x) = -x + 2c$. It should be clear that this is a bijection. To show that ϕ leaves the point c fixed, we compute $\phi(c) = -c + 2c = c$. We also want to show that ϕ is distance preserving (with the standard metric on the real line of absolute value) meaning that for $x, y \in \mathbb{R}$, $|x - y| = |\phi(x) - \phi(y)|$. To check this we compute $|\phi(x) - \phi(y)| = | - x + 2c + y - 2c| = |x - y|$.

b. We describe answers for parts b - d less formally. Symmetries of a point c in the plane include rotations centered at c, the identity map, and reflections about any line containing the point c.

c. Symmetries of a line segment in $\mathbb{R}$ include the identity map and reflections about the midpoint of the segment (this will map the given line segment to itself but will swap which side of the given line segment other distinct, disjoint line segments lie on).

d. Symmetries of a given line segment in the plane include the identity, integer multiples of a 180° rotation, reflections across the line containing the line segment, and reflections the perpendicular bisector of the line segment.

Definition A plane isometry ϕ has a **fixed point** if there exists a point in the plane P such that $\phi(P) = P$ (Although this notion was used in exercise 1 already without any formal definition).

11) Which types of plane isometries have exactly one fixed point.

(Answer) : Nonzero rotations about a point P have exactly one fixed point, namely the point P.

13) Which types of plane isometries have infinitely many fixed points.

(Answer) : The identity map and also reflections about a line L in the plane.

17) Do translations, together with the identity map, form a subgroup of the group of plane isometries?

(Answer) : Yes. First the composition of a translation with another translation is also a translation, so the set is closed under the composition. Associativity holds by the associativity of functions (translations are functions), which was shown in the first or second chapter. The identity element would just be the identity map and for any translation, we can reverse the translation (which is translation again), showing that inverses exist for any element of the set. So this set forms a group under the binary operation of composition.