Part III

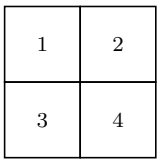
Pinter

Chapter 3

The Definition of Groups

Exercises

D. A Checkerboard Game



Our checkerboard has only 4 squares, numbered 1, 2, 3, and 4. There is a single checker on the board, and it has four possible moves:

V: Move vertically; that is, move from 1 to 3, or from 3 to 1, or form 2 to 4, or from 4 to 2.

H: Move horizontally; that is, move from 1 to 2 or vice versa, or from 3 to 4 or vice versa.

D: Move diagonally; that is, move from 2 to 3 or vice versa, or from 1 to 4 or vice versa.

I: Stay put.

We may consider an operation on the set of these four moves, which consists of performing moves successively. For example, if we move horizontally and then vertically, we end up with the same result as if we had moved diagonally:

$$H * V = D$$

If we perform two horizontal moves in succession, we end up where we started: $H * H = I$. And so on. If $G = \{V, H, D, I\}$, and $*$ is the operation we have just described, write the table of G. Granting associativity, explain why $\langle G, * \rangle$ is a group.

Chapter 4

Elementary Properties of Groups

7/19:

- Let G be a group, and let $a, b \in G$.

  Theorem 4.2. *If $ab = e$, then $a = b^{-1}$ and $b = a^{-1}$.*

Chapter 9

Isomorphism

7/20:

- **Isomorphism** (between groups G_1, G_2): A bijective function $f : G_1 \to G_2$ with the property that for any $a, b \in G_1$, $f(ab) = f(a)f(b)$. *Denoted by* $\boldsymbol{G_1 \cong G_2}$.

Exercises

A. Isomorphism Is an Equivalence Relation among Groups

1 Let G be any group. If $\varepsilon : G \to G$ is the identity function, $\varepsilon(x) = x$, show that ε is an isomorphism.

Proof. To prove that ε is an isomorphism, it will suffice to show that ε is a bijection and that $\varepsilon(ab) = \varepsilon(a)\varepsilon(b)$ for all $a, b \in G$. Let $a, b \in G$ be arbitrary. By the definition of ε, $\varepsilon(a) = \varepsilon(b)$ implies $a = b$. Thus, ε is injective. Additionally, we have that $\varepsilon(b) = b$, so ε is surjective. Therefore, it is bijective. Lastly,

$$\varepsilon(ab) = ab = \varepsilon(a)\varepsilon(b)$$

as desired. □

2 Let G_1, G_2 be groups, and $f : G_1 \to G_2$ be an isomorphism. Show that $f^{-1} : G_2 \to G_1$ is an isomorphism.

Proof. Since f is a bijection, f^{-1} exists and is a bijection. Additionally, let $c, d \in G_2$ be arbitrary. Then $f^{-1}(c) = a$ and $f^{-1}(d) = b$ for some $a, b \in G_1$. Thus, since $f(ab) = f(a)f(b) = cd$, we have that $f^{-1}(cd) = f^{-1}(f(ab)) = ab = f^{-1}(c)f^{-1}(d)$, as desired. □

3 Let G_1, G_2, G_3 be groups, and let $f : G_1 \to G_2$ and $g : G_2 \to G_3$ be isomorphisms. Prove that $g \circ f : G_1 \to G_3$ is an isomorphism.

Proof. Since f, g are bijections, $g \circ f$ is a bijection. Now let $a, b \in G_1$ be arbitrary. Thus, $f(ab) = f(a)f(b)$, where $f(a), f(b) \in G_2$. It follows that $g(f(a)f(b)) = g(f(a))g(f(b))$. Therefore,

$$(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b)$$

as desired. □

B. Elements Which Correspond under an Isomorphism

1 If e_1 denotes the neutral element of G_1 and e_2 denotes the neutral element of G_2, prove that $f(e_1) = e_2$.

Proof. For all $x \in G_1$, $e_1 x = x = x e_1$. Thus, by the definition of an isomorphism, $f(e_1)f(x) = f(e_1 x) = f(x)$ and $f(x)f(e_1) = f(x e_1) = f(x)$. It follows by their definition that $f(e_1)$ is a neutral element of G_2. Therefore, since neutral elements are unique, $f(e_1) = e_2$, as desired. □

2 Prove that for each element $a \in G_1$, $f(a^{-1}) = [f(a)]^{-1}$.

Proof. Let $a \in G_1$ be arbitrary. Then $e_2 = f(e_1) = f(aa^{-1}) = f(a)f(a^{-1})$. It follows by Theorem 4.2 that $f(a^{-1}) = [f(a)]^{-1}$, as desired. □

3 If G_1 is a cyclic group with generator a, prove that G_2 is also a cyclic group, with generator $f(a)$.

Proof. Suppose G_1 is a cyclic group of order n with generator a. We wish to show that G_2 is a cyclic group of order n with generator $f(a)$. By the definition of an isomorphism,

$$f(a^t) = f(\underbrace{aa\cdots a}_{t \text{ times}}) = \underbrace{f(a)f(a)\cdots f(a)}_{t \text{ times}} = f(a)^t$$

for all $t \in \mathbb{Z}$. As a special case, $e_2 = f(e_1) = f(a^n) = f(a)^n$, so G_2 is of order *at most* n. Now suppose for the sake of contradiction that there exists a positive integer $0 < t < n$ such that $f(a)^t = e_2$. Then $f(a^t) = e_2$, i.e., $a^t = e_2$. But this means that G_1 is of order t, a contradiction. □

C. Isomorphism of Some Finite Groups

1 G is the checkerboard game group of Chapter 3, Exercise D. H is the group of the complex numbers $\{i, -i, 1, -1\}$ under multiplication.

Proof. Suppose for the sake of contradiction that an isomorphism $f : G \to H$ exists. Since $-i^1 = -i$, $-i^2 = -1$, $-i^3 = i$, and $-i^4 = 1$, $H = \langle -i \rangle$. Thus, by Exercise 9.B.3, G is a cyclic group with generator $f^{-1}(-i)$. However, no element $x \in G$ suffices as a generator ($I^1 = I$, $V^2 = I$, $H^2 = I$, and $D^2 = I$), a contradiction. □

Chapter 13

Counting Cosets

7/22:

- **Left coset** (of H in G): The set of all products ah, where H is a subgroup of G, $a \in G$ is fixed, and h ranges over H. *Denoted by* $\boldsymbol{aH}$.
- **Right coset** (of H in G): The set of all products ha, where H is a subgroup of G, $a \in G$ is fixed, and h ranges over H. *Denoted by* $\boldsymbol{Ha}$.
- In this book, we choose to focus on right cosets.
- If $a \in Hb$, then $Ha = Hb$.

  Proof. Let $x \in Ha$ be arbitrary. Then there exists $h \in H$ such that $x = ha$. Similarly, since $a \in Hb$, there exists $h' \in H$ such that $a = h'b$. Thus, we have that $x = h(h'b) = (hh')b$ by the associative law. But since H is a subgroup of G, $hh' \in H$. Therefore, $x \in Hb$, as desired. The proof is symmetric in the other direction. □

- Let G be a group and let H be a fixed subgroup of G.

  Theorem 13.1. *The family of all the cosets Ha, as a ranges over G, is a partition of G.*

  Proof. To prove that the collection of all cosets of H is a partition of G, it will suffice to show that any two cosets are either disjoint or equal, and every element of G is in some coset. We take this one constraint at a time.

  Let Ha, Hb be arbitrary cosets of H in G. We divide into two cases (Ha, Hb are disjoint and Ha, Hb are not disjoint). If they are disjoint, we are done. On the other hand, if they are not disjoint, then there exists $x \in Ha \cap Hb$. Since $x \in Ha$, $x = h_1a$ for some $h_1 \in H$. Similarly, $x = h_2b$ for some $h_2 \in H$. It follows that $a = (h_1^{-1}h_2)b$. But since $h_1^{-1}h_2 \in H$ by the definition of a subgroup, the above fact implies that $Ha = Hb$, as desired.

  Let $x \in G$ be arbitrary. Since $e \in H$ by the definition of a subgroup, $x = ex \in Hx$, as desired. □

- Let G be a finite group, let H be be a fixed subgroup of G, and let $a \in G$ be arbitrary.

  Theorem 13.2. *If Ha is any coset of H, there is a one-to-one correspondence from H to Ha.*

  Proof. Let $f : H \to Ha$ be defined by $f(h) = ha$ for all $h \in H$. To prove that f is bijective, it will suffice to show that it is injective and surjective. To begin, let $f(h_1) = f(h_2)$. Then $h_1a = h_2a$. But by the cancellation law, $h_1 = h_2$, as desired. Now let $x \in Ha$ be arbitrary. By the definition of Ha, $x = ha$ for some $h \in H$. Therefore, $f(h) = ha = x$, as desired. □

  - This implies that if G is finite, all cosets of H have the same number of elements.

- Let G be a finite group, and H any subgroup of G.

Theorem 13.3 (Lagrange's Theorem)**.** *The order of G is a multiple of the order of H.*

Proof. By Theorem 13.1, we may let the cosets of H divide G into n partitions. By Theorem 2, each of these n partitions has the same cardinality $\text{ord}(H)$. Therefore, since the elements in the group are divided into n partitions of size $\text{ord}(H)$, $\text{ord}(G) = n\,\text{ord}(H)$, as desired. □

- Let G be a group.

  Theorem 13.4. *If G has a prime number p of elements, then G is a cyclic group. Furthermore, any element $a \neq e$ in G is a generator of G.*

  Proof. Let a be an arbitrary non-neutral element of G. As we know, $\langle a \rangle$ is a subgroup of G. Thus, by Lagrange's theorem, $\text{ord}(\langle a \rangle) \mid \text{ord}(G)$. However, since $\text{ord}(G) = p$ is prime, either $\text{ord}(\langle a \rangle) = 1$ or $\text{ord}(\langle a \rangle) = p$. But since $a \neq e$, $\text{ord}(\langle a \rangle) \neq 1$. Therefore, $\text{ord}(\langle a \rangle) = p$, and we have that G is a cyclic group with generator a, as desired. □

- Theorem 13.4 gives us complete information on all groups of prime order; in other words, every group of prime order is isomorphic to the well-behaved $\mathbb{Z}/p\mathbb{Z}$.

- Let G be a finite group and $a \in G$.

  Theorem 13.5. *The order of a divides the order of G.*

  Proof. Clearly, $\text{ord}(a) = \text{ord}(\langle a \rangle)$. But since $\langle a \rangle$ is a subgroup of G, Lagrange's theorem implies that $\text{ord}(\langle a \rangle) = \text{ord}(a) \mid \text{ord}(G)$, as desired. □

- **Index** (of H in G): The number of cosets of H in G. *Denoted by* $\boldsymbol{(G : H)}$.

- By Theorems 13.1 and 13.2,
$$(G : H) = \frac{\text{ord}(G)}{\text{ord}(H)}$$

Exercises

A. Examples of Cosets in Finite Groups

In parts 1-5, list the cosets of H. For each coset, list the elements of the coset.

1 $G = S_3$, $H = \{\epsilon, \beta, \delta\}$.

Answer.

$$H\epsilon = H\beta = H\delta = \{\epsilon, \beta, \delta\}$$
$$H\alpha = H\kappa = H\gamma = \{\alpha, \kappa, \gamma\}$$

□

2 $G = S_3$, $H = \{\epsilon, \alpha\}$.

Answer.

$$H\epsilon = H\alpha = \{\epsilon, \alpha\}$$
$$H\beta = H\gamma = \{\beta, \gamma\}$$
$$H\delta = H\kappa = \{\delta, \kappa\}$$

□

3 $G = \mathbb{Z}/15\mathbb{Z}$, $H = \langle 5 \rangle$.

Answer. If $H = \langle 5 \rangle$, then $H = \{0, 5, 10\}$. Therefore,

$$\begin{aligned} H + 0 = H + 5 = H + 10 &= \{0, 5, 10\} \\ H + 1 = H + 6 = H + 11 &= \{1, 6, 11\} \\ H + 2 = H + 7 = H + 12 &= \{2, 7, 12\} \\ H + 3 = H + 8 = H + 13 &= \{3, 8, 13\} \\ H + 4 = H + 9 = H + 14 &= \{4, 9, 14\} \end{aligned}$$

□

4 $G = D_4$, $H = \{R_0, R_4\}$.

Answer.

$$\begin{aligned} HR_0 = HR_4 &= \{R_0, R_4\} \\ HR_1 = HR_7 &= \{R_1, R_7\} \\ HR_2 = HR_5 &= \{R_2, R_5\} \\ HR_3 = HR_6 &= \{R_3, R_6\} \end{aligned}$$

□

5 $G = S_4$, $H = A_4$.

Answer. If $H = A_4$, then

$$\begin{aligned} H = \{&\left(\begin{smallmatrix}1&2&3&4\\1&2&3&4\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\1&3&4&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\1&4&2&3\end{smallmatrix}\right), \\ &\left(\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\2&3&1&4\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\2&4&3&1\end{smallmatrix}\right), \\ &\left(\begin{smallmatrix}1&2&3&4\\3&1&2&4\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\3&2&4&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right), \\ &\left(\begin{smallmatrix}1&2&3&4\\4&1&3&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\4&2&1&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\4&3&2&1\end{smallmatrix}\right)\} \end{aligned}$$ [1]

Therefore,

$$\begin{aligned} Hx = A_4 &\implies x \in A_4 \\ Hx = S_4 \setminus A_4 &\implies x \notin A_4 \end{aligned}$$

□

6 Indicate the order and index of each of the subgroups in parts 1-5.

Answer.
1: $\text{ord}(H) = 3$, $(G : H) = 2$.
2: $\text{ord}(H) = 2$, $(G : H) = 3$.
3: $\text{ord}(H) = 3$, $(G : H) = 5$.
4: $\text{ord}(H) = 2$, $(G : H) = 4$.
5: $\text{ord}(H) = 12$, $(G : H) = 2$. □

B. Examples of Cosets in Infinite Groups

Describe the cosets of the subgroups described in parts 1-5.

1 The subgroup $H = \langle 3 \rangle$ of $\mathbb{Z}$.

[1] For all $n \in \mathbb{N}$, $\text{ord}(S_n) = 2\,\text{ord}(A_n) = 2\,\text{ord}(S_n \setminus A_n)$. In A_n, there are $n!/n/2 = (n-1)!/2$ permutations that send $1 \mapsto 1$. In A_n, for all $m \in [n]$, there are an equal number of permutations that send $1 \to m$. Generalization of this one may be more complicated: In A_4, if $1 \mapsto m$ odd, then the remaining three numbers are an increasing cycle; similarly, if $1 \mapsto m$ even, then the remaining three numbers are a decreasing cycle. Relation to determinants of matrices? Minimum number of transpositions? – every permutation in A_4 can be written as the product of 0 or 2 transpositions. In general, the coset of any element in H is H.

Answer. If $x \in \langle 3 \rangle$, then $H + x = \langle 3 \rangle$.
If $x \in \{1 + n \mid n \in \langle 3 \rangle\}$, then $H + x = \{1 + n \mid n \in \langle 3 \rangle\}$.
If $x \in \{2 + n \mid n \in \langle 3 \rangle\}$, then $H + x = \{2 + n \mid n \in \langle 3 \rangle\}$. □

2 The subgroup $H = \mathbb{Z}$ of $\mathbb{R}$.

Answer. If $x \in \mathbb{R}$, let $\tilde{x}$ be the greatest integer less than or equal to x. Let $x \in \mathbb{R}$ Then $H + x = \{p \in \mathbb{R} \mid p - \tilde{p} = x - \tilde{x}\}$. □

3 The subgroup $H = \langle 2^n : n \in \mathbb{Z} \rangle$ of $\mathbb{R}^*$.

Answer. The coset of any element in H is H. Otherwise, its a scaled version of H. □

C. Elementary Consequence of Lagrange's Theorem

Let G be a finite group. Prove the following.

1 If G has order n, then $x^n = e$ for every $x \in G$.

Proof. $\langle x \rangle$ is a cyclic subgroup of G. Thus, $x^{\text{ord}(\langle x \rangle)} = e$. Additionally, by Lagrange's theorem, $\text{ord}(\langle x \rangle) \mid n$. Thus, let $n = m\,\text{ord}(\langle x \rangle)$. Therefore, $x^n = (x^{\text{ord}(\langle x \rangle)})^m = e^m = e$, as desired. □

2 Let G have order pq, where p, q are primes. Either G is cyclic, or every element $x \neq e$ in G has order p or q.

Proof. Let $x \in G$ such that $x \neq e$. We know that $\langle x \rangle$ is a cyclic subgroup of G, and that $\text{ord}(x) = \text{ord}(\langle x \rangle)$. Thus, by Lagrange's theorem, $\text{ord}(x) \mid pq$. This combined with the hypothesis that $x \neq e$ implies the $\text{ord}(x) \in \{p, q, pq\}$. We divide into two cases ($\text{ord}(x) = pq$, and $\text{ord}(x) \neq pq$). If $\text{ord}(x) = pq$, then G is cyclic with generator x, as desired. On the other hand, if $\text{ord}(x) = p$ or $\text{ord}(x) = q$, then every element $x \neq e$ in G has order p or q (for if one did not, it would have order pq; but then G would be cyclic, contradicting the fact that $\text{ord}(x) \in \{p, q\}$). □

E. Elementary Properties of Cosets

Let G be a group, and H a subgroup of G. Let a, b denote elements of G. Prove the following:

1 $Ha = Hb$ iff $ab^{-1} \in H$.

I. Conjugate Elements

If $a \in G$, a **conjugate** of a is any element of the form xax^{-1}, where $x \in G$. (Roughly speaking, a conjugate of a is any product consisting of a sandwiched between any element and its inverse.) Prove each of the following:

1 The relation "a is equal to the conjugate of b" is an equivalence relation in G. (Write $a \sim b$ for "a is equal to the conjugate of b.")

Proof. Criterion 1: Let $x = a$. Then $a = ae = aaa^{-1} = xax^{-1}$. Therefore, $a \sim a$.
Criterion 2: Let $a \sim b$. Then $a = xbx^{-1}$ for some $x \in G$. It follows that $b = x^{-1}ax = (x^{-1})a(x^{-1})^{-1}$. Therefore, $b \sim a$.
Criterion 3: Let $a \sim b$ and $b \sim c$. Then $a = xbx^{-1}$ and $b = ycy^{-1}$. It follows that $a = xycy^{-1}x^{-1} = (xy)c(xy)^{-1}$. Therefore, $a \sim c$. □

This relation $\sim$ partitions any group G into classes called **conjugacy classes**. (The conjugacy class of a is $[a] = \{xax^{-1} : x \in G\}$.)

For any element $a \in G$, the **centralizer** of a, denoted by C_a, is the set of all the elements in G which commute with a. That is,

$$C_a = \{x \in G \mid xa = ax\} = \{x \in G \mid xax^{-1} = a\}$$

Prove the following:

2 For any $a \in G$, C_a is a subgroup of G.

3 $x^{-1}ax = y^{-1}ay$ iff xy^{-1} commutes with a iff $xy^{-1} \in C_a$.

Proof. First, suppose that $x^{-1}ax = y^{-1}ay$. Then

$$axy^{-1} = xx^{-1}axy^{-1} = xy^{-1}ayy^{-1} = xy^{-1}a$$

as desired.

Second, suppose that xy^{-1} commutes with a. Then by the definition of the centralizer, $xy^{-1} \in C_a$.

Third, suppose that $xy^{-1} \in C_a$. Then $xy^{-1}ayx^{-1} = a$. Then $x^{-1}ax = x^{-1}xy^{-1}ayx^{-1}x = y^{-1}ay$, as desired. □

4 $x^{-1}ax = y^{-1}ay$ iff $C_ax = C_ay$.

Proof. Suppose first that $x^{-1}ax = y^{-1}ay$. Then by Exercise 13.I.3, $xy^{-1} \in C_a$. Therefore, by Exercise 13.E.1, $C_ax = C_ay$, as desired.

The proof is symmetric in the other direction. □

5 There is a one-to-one correspondence between the set of all the conjugates of a and the set of all the cosets of C_a.

J. Group Acting on a Set

Let A be a set, and let G be any subgroup of S_A. G is a group of permutations of A; we say it is a **group acting** (on the set A). Assume here that G is a finite group. If $u \in A$, the **orbit** (of u with respect to G) is the set

$$O(u) = \{g(u) : g \in G\}$$

1 Define a relation $\sim$ on A by $u \sim v$ iff $g(u) = v$ for some $g \in G$. Prove that $\sim$ is an equivalence relation on A, and that the orbits are its equivalence classes.

Proof. Criterion 1: Let u be an arbitrary element of A. Since G is a subgroup of S_A, G contains the identity permutation ϵ. Under this element of G, we know that $\epsilon(u) = u$. Therefore, $u \sim u$.

Criterion 2: Let $u \sim v$. Then there exists $g \in G$ such that $g(u) = v$. Since G is a subgroup of S_A, $g^{-1} \in G$. Thus, $g^{-1}(v) = g^{-1}(g(u)) = u$. Therefore, $v \sim u$.

Criterion 3: Let $u \sim v$ and $v \sim w$. Then there exist $g, h \in G$ such that $g(u) = v$ and $h(v) = w$. It follows that $(hg)(u) = h(g(u)) = w$. But since $hg \in G$ because G is closed under products, $u \sim w$.

To prove that the orbits are equivalence classes, it will suffice to show that any two orbits are either disjoint or equal. Let $O(u), O(v)$ be arbitrary orbits. If they are disjoint, we are done. However, if they are not, then there exists $w \in O(u) \cap O(v)$. It follows that $w = g(u) = h(v)$ for some $g, h \in G$. But then $w \sim u$ and $w \sim v$. It follows since $\sim$ is an equivalence relation that $u \sim v$. Thus, there exists $f \in G$ such that $f(u) = v$. □