

Modern Algebra Lecture Notes

Rebekah Dix

September 28, 2018

Contents

1	Group Theory	2
1.1	Basic Definitions/Examples	2
1.1.1	Symmetric Groups	4
1.1.2	Matrix Groups (General Linear Groups)	4
1.2	Subgroups	5
1.3	Homomorphisms	6
1.4	Cosets and Lagrange's Theorem	8
1.5	Cyclic Groups	11
2	Quizzes	12
2.1	Quiz 1	12
2.2	Quiz 2	12
2.3	Quiz 3	13
3	Homework Exercises	13
3.1	Homework 1	13
3.2	Homework 2	14
3.3	Homework 3	15
3.4	Homework 4	17
4	Honors Questions	17

1 Group Theory

1.1 Basic Definitions/Examples

Definition 1 (Group). A set G with a binary operation $\star : G \times G \rightarrow G$ is a group if the following axioms are satisfied:

1. *Associativity*: $(a \star b) \star c = a \star (b \star c)$ for every $a, b, c \in G$.
2. *Unit (or Identity)*: There exists an $e \in G$ such that $e \star a = a \star e = a$ for each a in G .
3. *Inverse*: For each $a \in G$ there is a $b \in G$ such that $a \star b = b \star a = e$.

Example 1 (Examples of Groups). The following are examples of groups.

1. $G = \mathbb{R} \setminus \{0\} = \mathbb{R}^*$ and $\star =$ multiplication.
2. $G = \mathbb{Z}$ and $\star =$ addition ($e = 0$ and $b = -a$).
3. $G = \{+1, -1\} \subset \mathbb{R}^*$ and $\star =$ multiplication.
4. $G = S_3 = \{ \text{All bijective functions } f : \{1, 2, 3\} \rightarrow \{1, 2, 3\} \}$ and $\star =$ composition of functions. To check the axioms in this example:
 - (a) *Associativity*: Holds because associativity is a basic property of composition
 - (b) *Unit Element*: The element that maps 1 to 1, 2 to 2, and 3 to 3 is the unit element. This element moves each element to itself.
 - (c) *Inverse*: S_3 is the set of bijections, so the definition of bijection implies there is an inverse by composition.

Definition 2 (Abelian/Commutative). A group G is *abelian* or *commutative* if $a \star b = b \star a$ for all $a \in G$.

Example 2. (Examples of Abelian Groups)

1. Examples 1, 2, and 3 above are Abelian. The commutativity follows from the commutativity of addition and multiplication.
2. Example 4 is not Abelian. It's easy to find a pair of elements that don't commute under composition.

Not everything is a group.

Example 3. (Non-Examples of Groups)

1. $G = \mathbb{R}$ and $\star =$ maximum. For example, $2 \star \pi = \max(2, \pi) = \pi$. Associativity is satisfied. The order in which we take the maximum of a set of elements doesn't matter – we'll eventually find the largest element regardless. However, there is no unit element. The reason is that there is no smallest element in \mathbb{R} .

2. $G = \mathbb{R}_{\geq 0}$ and $\star = \text{maximum}$. Associativity is satisfied. There is a unit element, namely 0 (observe that we've corrected the problem of not having a smallest element). Fix $g \in G$, and observe that $\max(g, 0) = \max(0, g) = g$. However, there need not be an inverse of each element. We can't take the maximum of some element $g > 0$ and 0 and get 0.

Claim 1. (The unit element is unique) Let G be a group and \star its binary operation. Suppose that $e_1, e_2 \in G$ are both units elements. Then, $e_1 = e_2$.

Proof. Since e_1 and e_2 are unit elements, we know that for all $a \in G$, $a \star e_1 = e_1 \star a = e_1$ and $a \star e_2 = e_2 \star a = e_2$. Consider the product $e_1 \star e_2$. We know that $e_1 \star e_2 = e_2$ since e_2 is a unit element. Further, $e_1 \star e_2 = e_1$ since e_1 is a unit element. Therefore, $e_1 = e_2$. \square

Lemma 1. (Cancellation Law) For every group G and $a, b, c \in G$ that satisfy $ab = ac$, we have $b = c$.

Proof. Let x be the inverse of a . Then, $x(ab) = x(ac)$. By associativity, we may write $(xa)b = (xa)c$. This simplifies to $1 \star b = 1 \star c$ or that $b = c$. \square

Corollary 1. (The inverse of a group element is unique) Let G be a group and let $a \in G$. If b and c are inverses of a , then $b = c$.

Proof. Since b and c are inverses of a , we know that $ab = 1 = ac$. Then by the Cancellation Law, we know $b = c$. \square

Exercise 1. Show that if $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Solution 1. Going back to the definition of a group and the axiom required to be an inverse element, we must show that $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = 1$. Then,

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1 \quad (1)$$

And,

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1} \cdot 1 \cdot b = b^{-1}b = 1 \quad (2)$$

Therefore, $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = 1$ so that $b^{-1}a^{-1}$ is the inverse of $(ab)^{-1}$.

Exercise 2. Give an example of $\tau \in S_3$ such that $\tau \neq 1$, $\tau^2 \neq 1$, and $\tau^3 \neq 1$.

Solution 2. Consider $\tau(1) = 2, \tau(2) = 3, \tau(3) = 1$. Then, $\tau^2(1) = 3$ and $\tau^3(1) = 1$. Thus is sufficient to show that $\tau \neq 1, \tau^2 \neq 1$, and $\tau^3 \neq 1$.

Definition 3. (The group $\mathbb{Z}/n\mathbb{Z}$) The group $\mathbb{Z}/n\mathbb{Z}$ is the set $\{0, 1, \dots, n-1\}$. That is, the possible (integer) remainders upon dividing by n . Recall that the remainder is the smallest number that you subtract from the original number so that it becomes divisible by n .

Exercise 3. Calculate $5 + 6 + 3$ in $\mathbb{Z}/7\mathbb{Z}$.

Solution 3. $5 + 6 + 3 = 14 \equiv 0 \pmod{7}$

Exercise 4. What is the inverse of 15 in $\mathbb{Z}/30\mathbb{Z}$.

Solution 4. Observe that $15 + 15 = 30 = 0$. Hence 15 is its own inverse.

Definition 4. (Order of a group, order of an element of a group) Let G be a group. We call $|G|$ the order of G (i.e. the number of elements in G). Further, the least $d > 0$ such that $g^d = 1$ is called the order of $g \in G$.

Example 4. (Orders of groups)

- $|S_n| = n!$
- $|\mathbb{Z}/n\mathbb{Z}| = n$

Exercise 5. Calculate the order of 2 in $\mathbb{Z}/7\mathbb{Z}$.

Solution 5. The order of 2 is 7.

1.1.1 Symmetric Groups

Definition 5. (Cycle, Cycle Decomposition, Length, k -Cycle) A cycle is a string of integers which represents the element of S_n which cyclically permutes these integers (and fixes all other integers). The product of all the cycles is called the cycle decomposition. The length of a cycle is the number of integers which appear in it. A cycle of length k is called a k -cycle.

1.1.2 Matrix Groups (General Linear Groups)

Example 5. Let $GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$ and let the binary operation be the multiplication of matrices. Let's check that the axioms are satisfied so that it is a group.

1. Associativity: Follows from basic properties of matrix multiplication.
2. Identity: Notice that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element.
3. Inverse: The condition $ad - bc \neq 0$ ensures that each element has an inverse.

For completeness, we also need to check that the product of two invertible matrices is again invertible (one quick proof of this uses the fact that taking a determinant is homomorphism. For instance $\det(A) = \det(A) \det(B)$, From this note that if both A and B have non-zero determinants, then AB also has a non-zero determinant). Also observe that this group is not abelian. More generally, for $n \geq 1$, we can define

$$GL_n(\mathbb{R}) = \left\{ n \times n \text{ matrix } A \mid \det A \neq 0 \right\} \quad (3)$$

1.2 Subgroups

Definition 6. (Subgroup) A subset H of a group G is called a subgroup of G if the following axioms are satisfied

1. Identity: $1 \in H$ (we could also write $1_G \in H$).
2. Closed under products: $h_1 h_2 \in H$ for all $h_1, h_2 \in H$ (in words, the binary operation of G applied to elements of H keeps products in H).
3. Closed under inverses: $h^{-1} \in H$ for all $h \in H$.

In this case we write $H \leq G$. Observe that H is indeed a group.

Example 6. (Examples of Subgroups)

1. Define $H = \{(123), (132), id\} \subset S_3$. Let's check the 3 axioms required to be a subgroup.
 - (a) Identity: Observe that $id \in H$.
 - (b) Closed under products: Define $\sigma = (123)$. Then $\sigma^2 = (132)$ and $\sigma^3 = id$. Therefore, $\sigma \circ \sigma^2 = \sigma^3 = id \in H$ and so forth.
 - (c) Closed under inverses: Observe that $(123)^{-1} = (321) = (132) \in H$.
2. Define $H = \{\lambda I_n | \lambda \in \mathbb{R} \setminus \{0\}\} \subset GL_n(\mathbb{R})$.
 - (a) Identity: Take $\lambda = 1$.
 - (b) Closed under products: Fix $\lambda_1, \lambda_2 \in \mathbb{R}^\times$. Then $(\lambda_1 I)(\lambda_2 I) = (\lambda_1 \lambda_2)I \in H$.
 - (c) Closed under inverses: Observe that $(\lambda I)^{-1} = \lambda^{-1}I \in H$.
3. Define $H = \{2, 4, 0\} \subset \mathbb{Z}/6\mathbb{Z}$.
 - (a) Identity: 0 is in the set.
 - (b) Closed under products: Note that $0 + 2 = 2 + 0 = 2 \in H$, $0 + 4 = 4 + 0 = 4 \in H$, and $2 + 4 = 4 + 2 = 0 \in H$.
 - (c) Closed under inverses: Note that $2^{-1} = 4 \in H$ (because $2 + 4 = 0$) and of course $4^{-1} = 2 \in H$.
4. Define $H = \{\sigma_n \in S_n | \sigma(n) = n\} \subset S_3$ (the set of n -permutations which fix the last index).
 - (a) Identity: $id \in H$ because the identity permutation fixes the last element.
 - (b) Closed under products: Let $\sigma, \tau \in H$. Then $\sigma \circ \tau(n) = \sigma(\tau(n)) = \sigma(n) = n$. Therefore $\sigma\tau$ also fixes the last element.
 - (c) Closed under inverses: Fix $\sigma \in H$. Since σ fixes n , it must also be that σ^{-1} fixes n . In words, σ takes n to n , so σ^{-1} must also take n to n .

Example 7. (Non-example of Subgroup) Define $H = \{\sigma \in S_3 | \sigma(1) \in \{1, 2\}\} \subset S_3$.

1. Identity: Satisfied.
2. Closed under products: Consider $\sigma = (123)$. Then $\sigma^2 = (132)$. But here, $\sigma(1) = 3$. Therefore this subset is not a subgroup.

1.3 Homomorphisms

Definition 7. (Homomorphism) Let G, H be groups. A function $\phi : G \rightarrow H$ is a homomorphism if for every $a, b \in G$, we have

$$\phi(ab) = \phi(a)\phi(b) \quad (4)$$

Note the the product ab on the left is computed in G and the product $\phi(x)\phi(y)$ is computed in H .

Example 8. (Examples of Homomorphisms)

1. Let $G = GL_n(\mathbb{R})$, $H = \mathbb{R}^\times$, $\phi : G \rightarrow H$. Define $\phi(A) = \det(A)$.
2. Let $G = \mathbb{Z}/7\mathbb{Z}$, $H = \{z \in \mathbb{C} : z^7 = 1\}$. Define

$$\phi(A) = e^{\frac{2\pi ia}{7}} \quad (5)$$

Then

$$\begin{aligned} \phi(ab) &= \phi(a + b) = e^{\frac{2\pi i(a+b-7k)}{7}} \\ &= e^{\frac{2\pi ia}{7}} e^{\frac{2\pi ib}{7}} e^{-2\pi ik} \\ &= e^{\frac{2\pi ia}{7}} e^{\frac{2\pi ib}{7}} \cdot 1 \\ &= \phi(a)\phi(b) \end{aligned}$$

Observe that ϕ is injective and surjective. ϕ is an isomorphism.

3. Define $\phi : G \rightarrow H$ for all $g \in G$, $\phi(g) = 1$.
4. Define $\phi : \mathbb{R}_{>0}^\times \rightarrow \mathbb{R}$, $\phi(x) = \log(x)$. Then

$$\phi(xy) = \log(xy) = \log(x) + \log(y) = \phi(x) + \phi(y) = \phi(x) \cdot \phi(y) \quad (6)$$

Claim 2. (Basic facts about homomorphisms) Let $\phi : G \rightarrow H$ be a homomorphism. Then

1. $\phi(1_G) = 1_H$ (the identity of G is mapped to the identity of H).
2. $\phi(x^{-1}) = \phi(x)^{-1}$ for all $x \in G$.

Proof. Observe that

1. $1 \cdot \phi(1) = \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$. Then the (right) cancellation law gives that $1 = \phi(1)$.
2. $\phi(x^{-1})\phi(x) = \phi(x^{-1}x) = \phi(1) = 1$ and $\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(1) = 1$. Therefore, by definition, $\phi(x^{-1}) = \phi(x)^{-1}$.

□

Example 9. (Example of facts about homomorphisms) Take $\sigma = (123) \in S_3$. Define $\phi : \mathbb{Z}/3\mathbb{Z} \rightarrow S_3$ by $\phi(t) = \sigma^t$. Then $\phi(0) = id$ (we expected this from the above claim), $\phi(1) = \sigma$, $\phi(2) = \sigma^2$.

Claim 3. Let $\phi : G \rightarrow H$ be a homomorphism. Then $Im(\phi) = \{\phi(g) | g \in G\} \leq H$.

Proof. Let's check the axioms required for $Im(\phi)$ to be a subgroup.

1. Identity: Take $1 \in G$, then $\phi(1) = 1 \in Im(\phi)$.
2. Closed under products: $\phi(a)\phi(b) = \phi(ab) \in Im(\phi)$.
3. Closed under inverses: $\phi(a) = \phi(a^{-1}) \in Im(\phi)$.

Therefore $Im(\phi)$ is a subgroup. □

Example 10. (The group $n\mathbb{Z}$) For $n \geq 1$, define $n\mathbb{Z} = \{k \in \mathbb{Z} : k \text{ is divisible by } n\}$. Observe that $n\mathbb{Z} \leq \mathbb{Z}$. Let's check the axioms:

1. Identity: $0 \in n\mathbb{Z}$ because 0 is divisible by everything.
2. Closed under products: If x, y are divisible by n , then xy will also be divisible by n .
3. Closed under inverses: If x is divisible by n , then $-x$ is divisible by n .

Example 11. (Another homomorphism) Define $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ by $\phi(k)$ is the remainder upon dividing k by n (clearly this remainder is in the set $\mathbb{Z}/n\mathbb{Z}$). Then ϕ is a homomorphism. We need to show that $\phi(a+b) = \phi(a) + \phi(b)$.

Observations about this example: Note that for each $k \in n\mathbb{Z}$, $\phi(k) = 0$. Moreover $\{k \in \mathbb{Z} : \phi(k) = 0\} = n\mathbb{Z}$. This motivates the following definition.

Definition 8. (Kernel) Let $\phi : G \rightarrow H$ be a homomorphism. Then

$$\ker(\phi) = \{g \in G : \phi(g) = 1\} \quad (7)$$

(note that 1 is the identity of H).

Claim 4. Let $\phi : G \rightarrow H$ be a homomorphism. Then $\ker(\phi) \leq G$. That is, the kernel of ϕ is a subgroup of G .

Proof. Let's check the 3 axioms required to be a subgroup:

1. Identity: Since ϕ is a homomorphism, we know that $\phi(1_G) = 1_H$. Therefore $1_G \in \ker(\phi)$.
2. Closed under products: Let $a, b \in \ker(\phi)$. We want to show that $ab \in \ker(\phi)$, which means that $\phi(ab) = 1$. Then

$$\phi(ab) = \phi(a)\phi(b) = 1 \cdot 1 = 1 \quad (8)$$

Therefore $ab \in \ker(\phi)$ so that $\ker(\phi)$ is closed under products.

3. Closed under inverses: Let $a \in \ker(\phi)$. Then

$$\phi(a^{-1}) = \phi(a)^{-1} = 1^{-1} = 1 \quad (9)$$

Therefore $a^{-1} \in \ker(\phi)$.

□

Example 12. (Examples of Kernels) The following are examples of kernels of homomorphisms:

1. The determinant is a homomorphism from $GL_n(\mathbb{R})$ to \mathbb{R}^\times . Then

$$\ker(\det) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\} \quad (10)$$

2. $\phi : S_3 \rightarrow \{\pm 1\}$ is a homomorphism. Define ϕ as

$$\begin{aligned} \phi(123) &= \phi(132) = 1 \\ \phi(12) &= \phi(13) = \phi(23) = -1 \\ \phi(id) &= 1 \end{aligned}$$

Then $\ker(\phi) = \{(123), (132), id\}$.

1.4 Cosets and Lagrange's Theorem

Example 13. (Equivalence Relation) Let G be a finite group and let $H \leq G$. Define a relation \sim on G by $a \sim b$ if and only if there exists an $h \in H$ such that $a = bh$. This condition also means that $ab^{-1} \in H$. We show that \sim is indeed an equivalence relation:

1. Reflexive ($\forall a \in G, a \sim a$): One way to see this is to recall that since H is a subgroup, we know that $aa^{-1} = 1 \in H$. Or simply, $a = a \cdot 1$ and $1 \in H$.
2. Symmetric ($\forall a, b \in G, a \sim b \implies b \sim a$): $a \sim b$ implies $b^{-1}a \in H$. We know that then $(b^{-1}a)^{-1} = a^{-1}b \in H$. Therefore $b \sim a$.

3. Transitive ($\forall a, b, c \in G, a \sim b, b \sim c \implies a \sim c$): $a \sim b$ implies $b^{-1}a \in H$ and $b \sim c$ implies $c^{-1}b \in H$. H is a subgroup, so it's closed under products. Thus $c^{-1}bb^{-1}a \in H$ or that $c^{-1}a \in H$. Therefore $a \sim c$.

Then let $[a] = \{b \in G | b \sim a\} = \{b \in G | \exists h \in H, b = ah\} = \{ah | h \in H\} = aH$. G can be written as a disjoint union of equivalence classes.

Definition 9. (Coset) Let $H \leq G$ and fixed $a \in G$. Let

$$aH = \{ah | h \in H\}$$

$$Ha = \{ha | h \in H\}$$

These sets are called a left coset and right coset of H in G . Write G/H for the set of left cosets $\{aH | a \in G\}$.

Example 14. (Cosets) If $a = 1$, then $aH = 1 \cdot H = H$. And, for any $a \in H$, $aH = H$: First observe that $aH \subset H$ since H is a subgroup. Indeed if $a, h \in H$, then $ah \in H$. Next we'll show $H \subset aH$. Fix $h \in H$. We want to show that $h \in aH$, or that it can be written in the form $a'h'$ where $h' \in H$. To achieve this, write $h = e \cdot h = a(a^{-1}h)$. Note that $a^{-1}h \in H$ since H is a subgroup. Therefore $h \in aH$. Together these equivalences show that $aH = H$ when $a \in H$.

Claim 5. (All left cosets of H have the same size) Let $H \leq G$ be groups and let $a \in G$. Then $|[a]| = |aH| = |H|$

Proof. We can give a bijection between the two sets to show they have the same number of elements. To that end, define $f : H \rightarrow aH$ by $f(h) = ah$.

1. f is injective: Fix $h_1, h_2 \in H$ such that $f(h_1) = f(h_2)$. Then $ah_1 = ah_2$. Use the left cancellation law see that $h_1 = h_2$.
2. f is surjective: We need to show that for all $h' \in aH$ there exists an $h \in H$ such that $f(h) = h'$. Consider $h = a^{-1}h'$. Then $f(a^{-1}h') = aa^{-1}h' = h'$.

Thus f is a bijection. This result of course implies that $|aH| = |bH| = |H|$ for all $a, b \in H$. In words, all left cosets of H have the same size as H . \square

Theorem 6. (Lagrange) Let G be a finite group and let $H \leq G$. Then $|H|$ divides $|G|$.

Proof. Using the above claim, define $f : H \rightarrow aH$ by $f(h) = ah$. Then it follows that $|[a]| = |aH| = |H|$. We can write G as a disjoint union of equivalence classes. Let k be the number of equivalence classes, and observe that they all have the same cardinality of as H . Therefore $|G| = k \cdot |H|$, so that $|H| \mid |G|$. \square

Definition 10. (Index) If G is a group (possibly infinite) and $H \leq G$, the number of left cosets of H in G is called the index of H in G and is denoted by $|G : H|$. Alternatively, $|G : H| = |G/H| = \{aH | a \in G\}$. If G is finite, the $|G : H| = \frac{|G|}{|H|}$.

Example 15. (Index when G finite) Let $G = S_3$ and $H = \{(123), (132), id\}$. H is a subgroup. Since G is finite, we can calculate the index of H in G as

$$|G : H| = \frac{|G|}{|H|} = \frac{6}{3} = 2 \quad (11)$$

Thus there are 2 left cosets of H in G . To write out G/H we need only find one other left coset other than the trivial coset. To do this, we can pick an element of G that is not in H . Then observe that

$$G/H = \{H, (12)H\} \quad (12)$$

You can verify that $(12)H = (13)G = (23)H$.

Example 16. (Index when G infinite) $\mathbb{R}_{>0} \subset \mathbb{R}^\times$. Then $|\mathbb{R}^\times : \mathbb{R}_{>0}| = 2$. Recall that this means that there are two left cosets of $\mathbb{R}_{>0}$ in \mathbb{R}^\times . We can enumerate these as follows

$$\mathbb{R}^\times / \mathbb{R}_{>0} = \{\mathbb{R}_{>0}, (-1) \cdot \mathbb{R}_{>0}\} \quad (13)$$

We can make an observation about the left cosets of $\mathbb{R}_{>0}$ more generally:

$$a\mathbb{R}_{>0} = \text{sgn}(a) \cdot \mathbb{R}_{>0} \quad (14)$$

Example 17. (Index of Permutation Group) As a slight abuse of notation, let S_3 be the set of permutations in S_4 for which the last index is fixed. Then, since S_3 is finite

$$|S_4 : S_3| = \frac{24}{6} = 4 \quad (15)$$

Therefore S_4/S_3 has 4 elements. To find the left cosets of S_3 in S_4 , look for elements of S_4 that aren't in S_3 . Intuitively, these are the permutations that *don't* fix 4. We can enumerate the left cosets as

1. $C_1 = \{\sigma \in S_4 | \sigma(4) = 4\}$ (this is the trivial coset)
2. $C_2 = \{\sigma \in S_4 | \sigma(4) = 3\}$
3. $C_3 = \{\sigma \in S_4 | \sigma(4) = 2\}$
4. $C_4 = \{\sigma \in S_4 | \sigma(4) = 1\}$

Note that we can write each of these cosets as (using C_2 as an example): τS_3 , where $\tau(4) = 3$. We can pick any such τ that satisfies this requirement, and the left cosets generated by the different choices of τ will be the same.

Definition 11. (Normal Subgroup) We say that a subgroup H of G is normal if $aH = Ha$ for every $a \in G$. Write $H \trianglelefteq G$. This means that the left and right cosets of a group are equivalent.

Example 18. (Non-example of a Normal Subgroup) Continuing the above example, let S_3 be the set of permutations in S_4 for which the last index is fixed [[Incomplete]].

Claim 6. (The Kernel of a Homomorphism is a Normal Subgroup) Let $\phi : G \rightarrow H$ be homomorphism. Then $\ker(\phi) \trianglelefteq G$.

Proof. Incomplete □

1.5 Cyclic Groups

Definition 12. (Cyclic Group) A group H is cyclic if H can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$. Write $H = \langle x \rangle$ and say H is generated by x .

An alternative definition is: Let G be a group and fix $x \in G$. Let H be the subset of G that contains all the powers of x . Then notice that $H = \{x^n \mid n \in \mathbb{Z}\}$ is a subgroup of G (the identity element must be in H since $x^0 = 1$, H is closed under products since adding exponents will keep us in H , and the inverse of x^n is x^{-n} , which is also in H). We call H the subgroup of G generated by x , $H = \langle x \rangle$, and H is cyclic.

Example 19. (Examples of Cyclic Groups)

1. Let $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$. Then

$$\langle x \rangle = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\} \quad (16)$$

You can see that taking positive powers of x continually increases the element in the upper-right hand corner. Finally, observe that

$$x^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad (17)$$

Therefore the powers of the inverse of x are also included in $\langle x \rangle$.

2. Let $x = 3 \in \mathbb{Z}/n\mathbb{Z}$. Then $\langle x \rangle = \{0, 3\}$.

Claim 7. (Every cyclic group is isomorphic to either \mathbb{Z} or to $\mathbb{Z}/n\mathbb{Z}$ for some $n \geq 1$.) For every group H for which there exists an $x \in H$ such that $H = \langle x \rangle$, there exists a bijective homomorphism (i.e. an isomorphism) $\phi : H \rightarrow C$ where $C = \mathbb{Z}$ or $C = \mathbb{Z}/n\mathbb{Z}$ for some $n \geq 1$.

Proof. There are two cases to consider.

1. The powers of x are distinct: Define $\phi : H \rightarrow \mathbb{Z}$ by $\phi(x^n) = n$. ϕ is bijective by construction. To check that ϕ is indeed a homomorphism, observe that

$$\phi(x^n \cdot x^m) = \phi(x^{n+m}) = n + m = \phi(x^n) + \phi(x^m) \quad (18)$$

2. The powers of x are not distinct: Suppose there is some $m \neq n$ such that $x^m = x^n$ (without loss of generality assume $m \leq n$). Then since $x^m = x^n$, we find that $x^m x^{-m} = x^n x^{-m}$. Therefore $x^{n-m} = 1$. Since there is some finite power of x that equals the identity, let k be the order of x . Define $\phi : \mathbb{Z}/k\mathbb{Z} \rightarrow \mathbb{Z}/k\mathbb{Z}$ by $\phi(x^r) = r$, where r is the remainder upon dividing r by k .

□

2 Quizzes

2.1 Quiz 1

Exercise 6. Give an example of $\sigma \in S_3$ such that σ has order 3.

Solution 7. Consider $\sigma = (123)$. Then $\sigma^2 = (132)$ and $\sigma^3 = (1)(2)(3)$. Therefore, $\sigma^1 \neq 1$, $\sigma^2 \neq 1$, but $\sigma^3 = 1$. Therefore, by definition, σ has order 3.

Exercise 7. Give an example of $\tau \in S_5$ such that τ has order 6.

Solution 8. Consider $\tau = (123)(45)$. Then $\tau^2 = (132)(4)(5)$, $\tau^3 = (1)(2)(3)(45)$, $\tau^4 = (123)(4)(5)$, $\tau^5 = (132)(45)$, $\tau^6 = (1)(2)(3)(4)(5)$.

2.2 Quiz 2

Exercise 8. Let $\tau \in S_6$. Show that

$$\tau \cdot (54132) \cdot \tau^{-1} = (\tau(5)\tau(4)\tau(1)\tau(3)\tau(2))$$

Solution 9. We can show this element by element. Observe that

$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(5)) = \tau \cdot (54132)(5) = \tau(4) \tag{19}$$

This shows that $\tau \cdot (54132) \cdot \tau^{-1}$ maps $\tau(5)$ to $\tau(4)$. Similarly,

$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(4)) = \tau \cdot (54132)(4) = \tau(1) \tag{20}$$

$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(1)) = \tau \cdot (54132)(1) = \tau(3) \tag{21}$$

$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(3)) = \tau \cdot (54132)(3) = \tau(2) \tag{22}$$

$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(2)) = \tau \cdot (54132)(2) = \tau(5) \tag{23}$$

Therefore $\tau \cdot (54132) \cdot \tau^{-1} = (\tau(5)\tau(4)\tau(1)\tau(3)\tau(2))$.

Exercise 9. Let G be a group and fix $g \in G$. Define $\phi : G \rightarrow G$ by $\phi(x) = gxg^{-1}$. Show ϕ is an isomorphism.

Solution 10. 1. ϕ is a homomorphism: Fix $x, y \in G$. Then

$$\begin{aligned}\phi(xy) &= g(xy)g^{-1} \\ &= gxg^{-1}gyg^{-1} \\ &= \phi(x)\phi(y)\end{aligned}$$

2. ϕ is injective: Fix $x, y \in G$, and suppose $\phi(x) = \phi(y)$. Then

$$\phi(x) = gxg^{-1} = gyg^{-1} = \phi(y) \quad (24)$$

Then use the right and left cancellation laws we get that $x = y$.

3. ϕ is surjective: Fix $y \in G$ and consider $x = g^{-1}yg$. Then

$$\phi(g^{-1}yg) = g(g^{-1}yg)g^{-1} = y \quad (25)$$

Therefore, for all $y \in G$, we can find an $x = g^{-1}yg$ such that $\phi(x) = y$.

2.3 Quiz 3

3 Homework Exercises

3.1 Homework 1

Exercise 10. Show that the group S_3 is not abelian.

Solution 11. To show that S_3 is not abelian, we must find an $a, b \in S_3$ such that $ab \neq ba$. To this end, consider the permutations $a(1) = 2, a(2) = 3, a(3) = 1$ and $b(1) = 1, b(2) = 3, b(3) = 2$. Then, $a(b(1)) = 2$ but $b(a(1)) = 3$. Therefore, $ab \neq ba$, so S_3 is not abelian.

Exercise 11. Is the set \mathbb{R} of real numbers with the binary operation of subtraction a group?

Solution 12. No. The associativity axiom fails. To see this, observe that $3 - (2 - 1) = 2$ but $(3 - 2) - 1 = 0$.

Exercise 12. Let G be a group, and take some $g \in G$. Show that the function f from G to itself defined by $f(x) = gx$ is injective (one-to-one).

Solution 13. Recall that f is injective if for all $a, b \in G, a \neq b$, we have that $f(a) \neq f(b)$. For the sake of reaching a contradiction, let $a, b \in G, a \neq b$, but suppose that $f(a) = f(b)$. Then $ga = gb$, by the definition of f . By the Cancellation Law, we must have that $a = b$, a contradiction.

Exercise 13. Give an example of $\sigma \in S_3$ such that $\sigma \neq 1$ and $\sigma\sigma \neq 1$.

Solution 14. Consider $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$. Then, $\sigma\sigma(1) = 3$. Therefore, $\sigma\sigma \neq 1$.

Exercise 14. Is the set of positive real numbers with the binary operation of multiplication a group?

Solution 15. Yes. Associativity follows from the associativity of the reals. The identity element is 1. Since we've excluded 0, each positive real does have an inverse.

Exercise 15. Show that the set $G = \{z \in \mathbb{C} : z^7 = 1\}$ is a group under multiplication.

Solution 16. We check each of the axioms:

1. Associativity: This follows from the associativity of \mathbb{C} .
2. Identity: Observe that $1 \in G$ since $1^7 = 1$. Fix $g \in G$, and under multiplication, $g \star 1 = 1 \star g = g$. Therefore, G has an identity.
3. Inverse: First observe that $0 \notin G$ since $0^7 = 0$. The inverse of $z \in G$ is simply z^{-1} . Since $z \in G$, we know that $z^7 = 1$. Then, $z^{-7} = 1^{-1} = 1$. Therefore, $z^{-1} \in G$ since $z^{-7} = 1$. Then $zz^{-1} = 1$, and the inverse of each $z \in G$ is also in G .
4. Closure of binary operation: Let $a, b \in G$, so that $a^7 = b^7 = 1$. Then $(ab)^7 = a^7 b^7 = 1$. Therefore $ab \in G$. (Remark: To show that $ab \in G$, we need to prove that $(ab)^7 = 1$. Therefore, in our proof, we can start with $(ab)^7$ directly.)

Exercise 16. Let G be a group in which $g^2 = 1$ for each $g \in G$. Show that G is abelian.

Solution 17. To show that G is abelian we must prove that for all $a, b \in G$, $ab = ba$. To that end, fix $a, b \in G$. Then $aabb = a^2b^2 = 1 \star 1 = 1 = (ab)^2 = abab$. Then by cancellation we have that $ab = ba$.

3.2 Homework 2

Exercise 17. How many elements does the group $S_3 \times \mathbb{Z}/5\mathbb{Z}$ have?

Solution 18. S_3 has $3! = 6$ elements. $\mathbb{Z}/5\mathbb{Z}$ has 5 elements. Thus $S_3 \times \mathbb{Z}/5\mathbb{Z}$ has $6 \times 5 = 30$ elements.

Exercise 18. Find the order of all elements in $\mathbb{Z}/10\mathbb{Z}$.

Solution 19. $|0| = 1$ (the order of an element is 1 iff that element is the identity). $|1| = 10$, $|2| = 5$, $|3| = 10$, $|4| = 5$, $|5| = 2$, $|6| = 5$, $|7| = 10$, $|8| = 5$, $|9| = 10$.

Exercise 19. What is the order of the permutation $(135)(26)(4798)$ in S_{10} ?

Solution 20. The order of a permutation is the lcm of the lengths of the cycles in its cycle decomposition. Here, the cycle lengths are 3, 2, and 4. Therefore the order of this permutation is 12.

Exercise 20. Let $\sigma \in S_n$ be a k -cycle, and let $\tau \in S_n$. Prove that $\tau\sigma\tau^{-1}$ is also a k -cycle.

Solution 21. Let $\sigma = (i_1 i_2 \dots i_k)$. We claim that $\tau\sigma\tau^{-1} = (\tau(i_1)\tau(i_2)\dots\tau(i_k))$. We can calculate each element of $\tau\sigma\tau^{-1}$ to show that this is true. Consider $\tau(i_1)$. Then,

$$\tau\sigma\tau^{-1}(\tau(i_1)) = \tau(\sigma(i_1)) = \tau(i_2) \quad (26)$$

Thus $\tau\sigma\tau^{-1}$ sends $\tau(i_1)$ to $\tau(i_2)$. A similar pattern holds for the other indices.

Exercise 21. Let $\sigma \in S_n$ be a k -cycle. Is σ^2 necessarily a k -cycle?

Solution 22. No. Consider this simple counterexample: (1234) . Then $\sigma^2 = (13)(24)$. σ^2 is not a k -cycle.

Exercise 22. Let G be a group, and let $g \in G$ be an element of order d . Show that the order of g^{-1} is also d .

Solution 23. There are two cases to consider. First suppose that $|g| = \infty$. For the sake of reaching a contradiction, suppose that $|g^{-1}| < \infty$. Thus for some $m < \infty$ we have that $(g^{-1})^m = 1$ (this is the smallest m for which this is true). But then,

$$g^m = g^{-1 \cdot m \cdot -1} = ((g^{-1})^m)^{-1} = 1^{-1} = 1 \quad (27)$$

This is a contradiction. Therefore if $|g| = \infty$, then $|g^{-1}| = \infty$. In the second case, we suppose that $|g| = d$ and $|g^{-1}| = c$. We then show that $c = d$. First,

$$(g^d)^{-1} = (g^{-1})^d = 1 \quad (28)$$

Therefore $c \leq d$. Next,

$$g^c = ((g^c)^{-1})^{-1} = ((g^{-1})^c)^{-1} = 1^{-1} = 1 \quad (29)$$

Therefore $d \leq c$. Together we get that $d = c$.

3.3 Homework 3

Exercise 23. Let G, H be groups, and let $\phi : G \times H \rightarrow G$ be the function defined by $\phi(g, h) = g$. Show that ϕ is a surjective homomorphism.

Solution 24. First show that ϕ is a homomorphism. To see this, fix $(g_1, h_1), (g_2, h_2) \in G \times H$. Then, $\phi(g_1 g_2, h_1 h_2) = g_1 g_2 = \phi(g_1, h_1) \phi(g_2, h_2)$. Thus ϕ is a homomorphism. Next show ϕ is surjective. That is, we must show that for all $g \in G$, there exists a $(g', h') \in G \times H$ such that $\phi(g', h') = g$. To see this, consider (g, h') . Then $\phi(g, h') = g$. By the same logic, ϕ is clearly not injective. Consider (g_1, h_1) and (g_1, h_2) where $h_1 \neq h_2$. But $\phi(g_1, h_1) = g_1 = \phi(g_1, h_2)$. This demonstrates an instance for which $a_1 \neq a_2$ but $\phi(a_1) = \phi(a_2)$.

Exercise 24. Let ϕ be the function which maps every $A \in GL_n(\mathbb{R})$ to the transpose of its inverse. Show that ϕ is an isomorphism from $GL_n(\mathbb{R})$ to itself.

Solution 25. First show ϕ is a homomorphism. Fix $A, B \in GL_n(\mathbb{R})$. Then

$$\begin{aligned}\phi(AB) &= ((AB)^{-1})^T \\ &= (B^{-1}A^{-1})^T \\ &= (A^{-1})^T(B^{-1})^T \\ &= \phi(A)\phi(B)\end{aligned}$$

Next show ϕ is injective. That is, we will show that $\phi(A) = \phi(B)$ implies $A = B$. Then

$$\phi(AB) = \phi(A)\phi(B) = \phi(A)\phi(A)$$

Thus

$$(A^{-1})^T(B^{-1})^T = (A^{-1})^T(A^{-1})^T \quad (30)$$

Use the right left cancellation law to show that $(B^{-1})^T = (A^{-1})^T$. This implies that $A = B$. Next show ϕ is surjective. That is, we must show that for all $B \in GL_n(\mathbb{R})$ there exists an $A \in GL_n(\mathbb{R})$ such that $\phi(A) = B$. Consider $A = (B^T)^{-1}$. Then

$$\phi((B^T)^{-1}) = (((B^T)^{-1})^{-1})^T \quad (31)$$

$$= B \quad (32)$$

Therefore ϕ is an isomorphism.

Exercise 25. Let p be a prime number, and let G be a group of order p . Show that G has exactly two distinct subgroups.

Solution 26. Lagrange's Theorem tells us that if H is a subgroup of G , then $|H|$ divides $|G|$. Therefore the only possible orders for subgroups of G are 1 and p . Now note that G can only have one subgroup of order 1. This follows because the identity element must be in every subgroup. Next note that no subgroup can have an order greater than p since a subgroup must be a subset of G . Clearly the only subgroup of G with order p is G itself.

Exercise 26. Show that $H = \{\sigma \in S_5 : \{\sigma(1), \sigma(2)\} = \{1, 2\}\} \leq S_5$, count the number of elements in it, and verify that Lagrange's theorem holds in this case.

Solution 27. It's fairly clear that H is a subgroup of G . Then, the number of elements in H is $2! \times 3! = 12$. The number of elements in $S_5 = 5! = 120$. Observe that $120/12 = 10$. Thus Lagrange's theorem holds.

Exercise 27. Let A be an abelian group, and define $\phi : A \rightarrow A$ by $\phi(a) = a^2$. Show that ϕ is a homomorphism.

Solution 28. Fix $a, b \in G$. Then

$$\begin{aligned}
 \phi(ab) &= (ab)^2 \\
 &= (ab)(ab) \\
 &= a^2b^2 && \text{(since } A \text{ is abelian)} \\
 &= \phi(a)\phi(b)
 \end{aligned}$$

Exercise 28. Let G, H be groups, and let $\phi : G \rightarrow H$ be a homomorphism. Show that ϕ is injective if and only if $\ker(\phi) = \{1\}$.

Solution 29. First suppose ϕ is injective. Since ϕ is a homomorphism, the identity element e of G is mapped to the identity element e' of H . Thus $\phi(e) = e'$. Let $g \in \ker(\phi)$. By definition $\phi(g) = e'$. Thus since ϕ is injective, we have that $\phi(e) = \phi(g)$ implies that $e = g$. Therefore the kernel is trivial.

Now suppose $\ker(\phi) = \{1\}$. Fix $g_1, g_2 \in G$ such that $\phi(g_1) = \phi(g_2)$. Then

$$\begin{aligned}
 \phi(g_1g_2^{-1}) &= \phi(g_1)\phi(g_2^{-1}) && (\phi \text{ is a homomorphism}) \\
 &= \phi(g_1)\phi(g_2)^{-1} && \text{(property of homomorphism)} \\
 &= \phi(g_1)\phi(g_1)^{-1} && \text{(since } \phi(g_1) = \phi(g_2)) \\
 &= 1
 \end{aligned}$$

Therefore $g_1g_2^{-1} \in \ker(\phi)$. Since we assumed $\ker(\phi) = \{1\}$, it must be that $g_1g_2^{-1} = 1$. This implies that $g_1 = g_2$.

3.4 Homework 4

4 Honors Questions

Exercise 29. From homework 1, we showed that if $g^2 = 1$ for all $g \in G$ where G is a group, then G is abelian. Note that $ab = ba$ iff $aba^{-1}b^{-1} = 1$. Can we write $aba^{-1}b^{-1}$ as a product of squares $c_1c_2c_3 \dots$? (And then each $c_i^2 = 1$).

Solution 30.