# Schaum's Outline of Abstract Algebra Notes and Exercises

Jasper Ty

# Contents

# Part I

# Sets and Relations

# Chapter 1

# Sets

I don't have much to write here as far as notes go.

## Exercises

**Q1.1.** Exhibit in tabular form:

(a) $A = \{a : a \in \mathbb{N}, 2 < a < 6\}$

(b) $B = \{p : p \in \mathbb{N}, p < 10, p \text{ is odd}\}$

(c) $C = \{x : x \in \mathbb{Z}, 2x^2 + x - 6 = 0\}$

**A1.1.**

(a) $A = \{3, 4, 5\}$

(b) $B = \{9, 7, 5, 3, 1\}$

(c) $C = \{-2\}$

**Q1.2.** Let $A = \{a, b, c, d\}$, $B = \{a, c, g\}$, $C = \{c, g, m, n, p\}$. Then $A \cup B = \{a, b, c, d, g\}$, $A \cup C = \{a, b, c, d, g, m, n, p\}$, $B \cup C = \{a, c, g, m, n, p\}$;

**A1.2. WHAT IS THE QUESTION?**

**Q1.3.** Consider the subsets $K = \{2, 4, 6, 8\}$, $L = \{1, 2, 3, 4\}$, $M = \{3, 4, 5, 6, 8\}$ of $U = \{1, 2, 3, \ldots, 10\}$.

(a) Exhibit $K'$, $L'$, $M'$ in tabular form.

(b) Show that $(K \cup L)' = K' \cap L'$

**A1.3.**

(a) $K' = \{1, 3, 5, 7, 9, 10\}$
$L' = \{5, 6, 7, 8, 9, 10\}$
$U' = \{1, 2, 7, 9, 10\}$

(b) $K \cup L = \{1, 2, 3, 4, 6, 8\}$, so $(K \cup L)' = \{5, 7, 9, 10\}$. Using the above, $K' \cap L' = \{5, 7, 9, 10\}$.

**Q1.4.** Skip
**Q1.5.** Skip

**Q1.6.** Skip

**Q1.7.** Skip

**Q1.8.** Prove $(A \cup B) \cup C = A \cup (B \cup C)$

**A1.8.** Any element $x$ belongs to the left hand side if $(x \in A \vee x \in B) \vee x \in C$. It belongs to the right hand side if $x \in A \vee (x \in B \vee x \in C)$. Both expressions are logically equivalent. Then the left set is equal to the right set by the axiom of extensionality.

**Q1.9.** Prove $(A \cap B) \cap C = A \cap (B \cap C)$

**A1.9.** Similar answer as the previous– follows from the associativity of $\wedge$

**Q1.10.** Prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

**A1.10.** Follows from $\wedge$ distributing over $\vee$

**Q1.11.** Prove $(A \cap B)' = A' \cap B'$

**A1.11.** Follows from DeMorgan's laws

**Q1.12.** Prove $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

**A1.12.** Follows from $\vee$ distributing over $\wedge$

**Q1.13.** Prove $A - (B \cup C) = (A - B) \cap (A - C)$

**A1.13.** Follows again from DeMorgan's laws (for classical logic): $x$ belongs to the left hand side if

$$x \in A \wedge \neg(x \in B \vee x \in C)$$

Which is equivalent to

$$x \in A \wedge (x \notin B \wedge x \notin C)$$

Then, since $\wedge$ distributes over itself, we can rewrite this as

$$(x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)$$

Which is the right hand side.

**Q1.14.** Prove: $(A \cup B) \cap B' = A$ if and only if $A \cap B = \varnothing$

**A1.14.** By distributivity,

$$B' \cap (A \cup B) = (B' \cap A) \cup (B' \cap B)$$

Then,

$$(B' \cap A) \cup (B' \cap B) = (B' \cup A) \cap \varnothing = B' \cap A \ = A - B$$

Hence the equation is equivalent to

$$A - B = A$$

Which is only true if and only if $A \cap B = \varnothing$

**Q1.15.** Prove that $X \subseteq Y$ if and only if $Y' \subseteq X$

**A1.15.** $X \subseteq Y$ when $a \in X \implies a \in Y$. By contraposition, this is equivalent to $a \notin Y \implies a \notin X$, which is the definition of $Y' \subseteq X'$

**Q1.16.** Prove the identity $(A-B) \cup (B-A) = (A \cup B) - (A \cap B)$ of Example 10 using the identity $A - B = A \cap B'$ of Example 9

**A1.16.**

$$\begin{aligned}
(A \cup B) - (A \cap B) &= (A \cup B) \cap (A \cap B)' \\
&= (A \cup B) \cap (A' \cup B') \\
&= ((A \cup B) \cap A') \cup ((A \cup B) \cap B') \\
&= ((A \cap A') \cup (B \cap A')) \cup ((A \cap B') \cup (B \cap B')) \\
&= (\varnothing \cup (B - A)) \cup ((A - B) \cup \varnothing) \\
&= (A - B) \cup (B - A)
\end{aligned}$$

**Q1.17.** In Fig. 1-8, show that any two line segments have the same number of points.

**A1.17.** Book has a geometric solution.

**Q1.18.** Prove:

(a) $x \to x + 2$ is a mapping of $\mathbb{N}$ into, but not onto, $\mathbb{N}$.

(b) $x \to 3x - 2$ is a one-to-one mapping of $\mathbb{Q}$ onto $\mathbb{Q}$

(c) $x \to x^3 - x^2 - x$ is a mapping of $\mathbb{R}$ onto $\mathbb{R}$ but not one-to-one.

**A1.18.**

(a) By the cancellation law in $\mathbb{N}$, $x + 2 = y + 2$ implies $x = y$, so the map is injective. But there is no natural number $x$ such that $x + 2 = 1$. Hence the map cannot be onto.

(b) By the cancellation laws again for $\mathbb{Q}$, $3x-2 = 3y-2$ imply $x = y$, so this map is into. Moreover, for all $h \in \mathbb{Q}$, the map sends the number $(h + 2)/3$ to $h$, hence the map is surjective.

(c) The map is equivalent to

$$x \to (x)(x - \phi^+)(x - \phi^-)$$

where $\phi^+$ and $\phi^-$ are the roots to the equation $x^2 - x - 1 = 0$. Hence the map is not injective, as multiple $x$ map to 0. The map is surjective, because the equation $x^3 - x^2 - x - r = 0$ always has a real root.

**Q1.19.** Prove: If $\alpha$ is a one-to-one mapping of a set $S$ onto a set $T$, then $\alpha$ has a unique inverse and conversely.

**A1.19.** Suppose $\alpha$ is one-to-one. Let $t \in T$. There must exist $s \in S$ such that $\alpha(s) = t$, since $\alpha$ is onto. Suppose another such element $s' \in S$ existed, then $\alpha(s') = t = \alpha(s)$, so it must be that $s = s'$, hence $s$ is unique. Define $a^{-1}(t) = s$ for all $t \in T$. Then $\alpha \circ \alpha^{-1} = \text{id}$.

$\alpha$ must be unique, since inverse elements in any binary operation are unique.

**Q1.20.** Prove: If $\alpha$ is a one-to-one mapping of a set $S$ onto a set $T$ and $\beta$ is a one-to-one mapping of $T$ onto a set $U$, then $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$

**A1.20.**

## Supplementary Problems

**Q1.21.** Exhibit each of the following in tabular form:

**A1.21.**

# Chapter 2

# Relations and Operations

# Part II

# Number Systems

# Chapter 3

# The Natural Numbers

# Chapter 4

# The Integers

# Chapter 5

# Some Properties of Integers

# Chapter 6

# The Rational Numbers

# Chapter 7

# The Real Numbers

# Chapter 8

# The Complex Numbers

# Part III

# Groups, Rings, and Fields

# Chapter 9

# Groups

## 9.1 Groups

**DEFINITION 9.1:** A non-empty set $\mathcal{G}$ equipped with a binary operation $\circ$ is a *group* if

**P**$_1$: $(a \circ b) \circ c = a \circ (b \circ c)$ (Associativity)

**P**$_2$: There exists an element $1 \in \mathcal{G}$ such that $1 \circ a = a \circ 1 = a$ for all $a \in \mathcal{G}$ (Unit)

**P**$_3$: For all $a \in \mathcal{G}$, there exists an element $a^{-1}$ such that $a \circ a^{-1} = a^{-1} \circ a = 1$ (Inverse)

**EXAMPLE 1**

(a) The set $\mathbb{Z}$ of all integers. $+$ is the operation, 0 is the identity element and the inverse of $a$ is $-a$. This is the *additive group* $\mathbb{Z}$.

(b)

## 9.2 Simple Properties of Groups

**THEOREM I.** (Left Cancellation)
Let $a, b, c \in \mathcal{G}$. Then $a \circ b = a \circ c$ implies $b = c$.

**THEOREM II.** (Latin Square Property)
Let $a, b \in \mathcal{G}$, then the equations

$$ax = b$$

$$ya = b$$

have unique solutions $x$ and $y$ respectively.

**THEOREM III.** (Involution)
For all $a \in \mathcal{G}$, $(a^{-1})^{-1} = a$.

**THEOREM IV.**
Let $a, b \in \mathcal{G}$. Then $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

**THEOREM V.** (Inverse of composition is reversed composition of inverse)
Let $a, b, \ldots, p, q \in \mathcal{G}$, then

$$(a \circ b \circ \cdots \circ p \circ q)^{-1} = p^{-1} \circ q^{-1} \circ \cdots \circ b^{-1} \circ a^{-1}$$

**THEOREM VI.** For all $a \in \mathcal{G}$ and $m, n \in \mathbb{Z}$,

$$a^m \circ a^n = a^{m+n}$$

$$(a^m)^n = a^{mn}$$

**DEFINITION 9.2:** The *order of a group* $\mathcal{G}$ is the number of elements in $\mathcal{G}$.

**DEFINITION 9.3:** The *order of an element* $a \in \mathcal{G}$ is the least positive integer $n$ such that $a^n = 1$.

**DEFINITION 9.4:** If $a \in \mathbb{Z}$ is not 0, then the order of $a$ is infinite.

## 9.3 Subgroups

**DEFINITION 9.5:** Let $\mathcal{G}$ be a group with the operation $\circ$. A subset $\mathcal{H}$ of $\mathcal{G}$ is a *subgroup of* $\mathcal{G}$ if $\mathcal{H}$ is also a group with the operation $\circ$ (restricted to $\mathcal{H}$).

Every group $\mathcal{G}$ has two trivial subgroups: $\{1\}$ and $G$.

**THEOREM VII.** $\mathcal{G}'$ is a subgroup of $\mathcal{G}$ if and only if

(i) $a, b \in \mathcal{G}'$ implies $a \circ b \in \mathcal{G}'$

(ii) $a \in \mathcal{G}'$ implies $a^{-1} \in \mathcal{G}'$

**THEOREM VIII.** $\mathcal{G}'$ is a subgroup of $\mathcal{G}$ if and only if $a, b \in \mathcal{G}'$ implies $a^{-1} \circ b \in \mathcal{G}'$

**THEOREM IX.** $\{a^n : n \in \mathbb{Z}\}$ is a subgroup of $\mathcal{G}$ for all $a \in \mathcal{G}$

**THEOREM X.** The intersection of any set of subgroups of $\mathcal{G}$ is a subgroup of $\mathcal{G}$.

## 9.4 Cyclic groups

**DEFINITION 9.6:** A group is *cyclic* if it is generated by a single element $a$.

**THEOREM XI.** If $\mathcal{G}$ is a cyclic group of order $n$ generated by $a$ then $a^t$ is a generator of $\mathcal{G}$ if and only if $\gcd(n, t) = 1$

**THEOREM XII.** Every subgroup of a cyclic group is cyclic.

## 9.5 Permutation groups

$S_n$ is the symmetric group.

## 9.6 Homomorphisms

**DEFINITION 9.7:** If $\mathcal{G}$ is a group with operation $\circ$ and $\mathcal{H}$ is a group with operation $\Box$, a homomorphism between $\mathcal{G}$ and $\mathcal{H}$ is a function $\phi : \mathcal{G} \to \mathcal{H}$ such that for all $a, b \in \mathcal{G}$,

$$\phi(a \circ b) = \phi(a) \Box \phi(b)$$

**THEOREM XIII.** Letting $\mathcal{G}$, $\mathcal{H}$, and $\phi$ be defined as above, $\phi(1_{\mathcal{G}}) = 1_{\mathcal{H}}$ and $\phi(a^{-1}) = \phi(a)^{-1}$ for all $a \in \mathcal{G}$.

**THEOREM XIV.** The homomorphic image of a cyclic group is cyclic

## 9.7 Isomorphisms

**DEFINITION 9.8:** If $\phi$ happens to also be a bijection of sets, then $\phi$ is called an *isomorphism* and $\mathcal{G}$ and $\mathcal{H}$ are said to be *isomorphic*

**THEOREM XV.**

(a) Every cyclic group of infinite order is isomorphic to $\mathbb{Z}$

(b) Every cyclic group of order n is isomorphic to $\mathbb{Z}_n$

**THEOREM XVI.** (Cayley's Theorem) Every finite group of order $n$ is isomorphic to a subgroup of $S_n$

## 9.8 Cosets

**DEFINITION 9.9:** Let $\mathcal{G}$ be a finite group with operation $\circ$, $H$ be a subgroup of $\mathcal{G}$,and $a \in \mathcal{G}$. The *right coset of $H$ generated by $a$* $Ha$ is

$$Ha := \{h \circ a : h \in H\}$$

Similarly, the *left coset of $H$ generated by $a$* is

$$aH := \{a \circ h : h \in H\}$$

## Exercises

**Q9.1.** Does $\mathbb{Z}_3$, the set of residue classes modulo 3, form a group with respect to addition? with respect to multiplication?

**A9.1.** Yes, with respect to addition. No, with respect to multiplication. It can be checked exhaustively.

| $+$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| $\times$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

**Q9.2.** Do the non-zero residue classes modulo 4 form a group with respect to multiplication?

**A9.2.** No it is not a group. 2 has no inverse modulo 4.

**Q9.3.** Prove: If $a, b, c \in \mathcal{G}$, then $a \circ b = a \circ c$ (also, $b \circ a = c \circ a$) implies $b = c$

**A9.3.** Multiply on the left by $a^{-1}$. (For the right case, multiply on the right)

**Q9.4.** Prove: When $a, b \in \mathcal{G}$, each of the equations $a \circ x = b$ and $y \circ a = b$ has a unique solution.

**A9.4.** $x = a^{-1} \circ b$ and $y = b \circ a^{-1}$ are solutions. That they are unique follows from the cancellation property; if $x$ and $x'$ are solutions, then $a \circ x = a \circ x'$, hence $x = x'$.

**Q9.5.** Prove: For any $a \in \mathcal{G}$, $a^m \circ a^n = a^{m+n}$ when $m, n \in \mathbb{Z}$ **A9.5.** -

**Q9.6.** Prove: A non-empty subset $\mathcal{G}'$ of a group $\mathcal{G}$ is a subgroup of $G$ if and only if, for all $a, b \in \mathcal{G}'$, $a^{-1} \circ b \in \mathcal{G}'$

**A9.6.** Let $b = 1$. Then the condition shows that $a^{-1} \in \mathcal{G}'$ for all $a \in \mathcal{G}'$. That then implies that $(a^{-1})^{-1} \circ b \in \mathcal{G}'$, so we recover the closure condition $a, b \in \mathcal{G}'$ implies $a \circ b \in \mathcal{G}'$. Hence $\mathcal{G}'$ is a subgroup of $\mathcal{G}$.

**Q9.7.** Prove: If $S$ is any set of subgroups of a group $\mathcal{G}$, the intersection of these subgroups is also a subgroup of $\mathcal{G}$.

**A9.7.** Let $\mathcal{H} = \bigcap S$. Let $a \in \mathcal{H}$. Then $a^{-1}$ exists in every subgroup in $S$. Hence $a^{-1} \in \mathcal{H}$. Let $a, b \in \mathcal{H}$. Then, again, $a \circ b$ is in every subgroup of $S$. Then $a \circ b \in mathcalH$. Then $\mathcal{H}$ is a subgroup of $\mathcal{G}$.

**Q9.8.** Prove: Every subgroup of a cyclic group is itself a cyclic group.

**A9.8.** Let $\mathcal{G}$ be a cyclic group and $\mathcal{H}$ be a subgroup of $\mathcal{G}$. Consider the element $a^m \in \mathcal{H}$ with the least positive $m$. Then take any other element $a^k \in \mathcal{H}$. Then use Euclidean division to find $k = mq + r$. Then

$$a^k = a^{mq+r} = (a^m)^q \circ a^r$$

Then

$$(a^m)^{-q} \circ a^k = a^r$$

Since $a^m \in \mathcal{H}$, $(a^m)^{-q} \in \mathcal{H}$. Then, since $a^k \in \mathcal{H}$ by assumption, $a^r \in \mathcal{H}$. But since $r < m$, $r$ must equal 0, hence $a^k = (a^m)^q$, and $\mathcal{H}$ is generated by $a^m$

**Q9.9.** The subset $\{\mathbf{u}, \rho\}$

# Chapter 10

# Further Topics on Group Theory

## 10.1 Further Topics on Group Theory

# Chapter 11

# Rings

## 11.1 Rings

**DEFINITION 11.1:** A non-empty set $\mathcal{R}$ is a *ring* if it satisfies

## 11.2 Properties of Rings

## 11.3 Subrings

# Chapter 12

# Integral Domains, Division Rings, and Fields

# Chapter 13

# Polynomials

# Chapter 14

# Vector Spaces

# Chapter 15

# Matrices

# Chapter 16

# Matrix Polynomials

# Chapter 17

# Linear Algebras

## Chapter 18

# Boolean Algebras