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 ϕ^+ and ϕ^- 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 α is a one-to-one mapping of a set S onto a set T, then α has a unique inverse and conversely.

A1.19. Suppose α is one-to-one. Let $t \in T$. There must exist $s \in S$ such that $\alpha(s) = t$, since α 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 $\alpha \circ \alpha^{-1} = \text{id}$.

α must be unique, since inverse elements in any binary operation are unique.

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

A1.20. $\alpha\beta\beta^{-1}\alpha^{-1} = \text{id}$

Supplementary Problems

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

(a) the set of negative integers greater than -6

(b) the set of integers between -3 and 4,

(c) the set of integers whose squares are less than 20,

(d) the set of all positive factors of 18,

(e) the set of all common factors of 16 and 24,

(f) $\{p : p \in \mathbb{N}, p^2 < 10\}$

(g) $\{b : b \in \mathbb{N}, 3 \leq b \leq 8\}$

(h) $\{x : x \in \mathbb{Z}, 3x^2 + 7x + 2 = 0\}$

(i) $\{x : x \in \mathbb{Q}, 2x^2 + 5x + 3 = 0\}$

A1.21.

(a) $\{-5, -4, -3, -2, -1\}$

(b) $\{-2, -1, 0, 1, 2, 3\}$

(c) $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$

(d) $\{1, 2, 3, 6, 9, 18\}$

(e) $\{1, 2, 4, 8\}$

(f) $\{1, 2, 3\}$

(g) $\{3, 4, 5, 6, 7, 8\}$

(h) $3x^2 + 7x + 2 = (3x + 1)(x + 2)$, so the roots are -2 and $-1/3$. So our set in tabular form is $\{-2\}$

(i) $2x^2 + 5x + 3 = (2x + 3)(x + 1)$, so the roots are $-3/2$ and -1. So our set in tabular form is $\{-3/2, -1\}$

Q1.22. Verify:

(a) $\{x : x \in \mathbb{N}, x < 1\} = \varnothing$

(a) $\{x : x \in \mathbb{Z}, 6x^2 + 5x - 4\} = \varnothing$

A1.22.

(a) $x \geq 1$ for all $x \in \mathbb{N}$.

(a) $6x^2 + 5x - 4 = (3x + 4)(2x - 1)$. So the roots are $1/2$ and $-4/3$, which are non-integers.

Q1.23. Exhibit the 15 proper subsets of $S = \{a, b, c, d\}$

A1.23. $\varnothing$, $\{a\}$, $\{b\}$, $\{c\}$, $\{d\}$, $\{a, b\}$, $\{a, c\}$, $\{a, d\}$, $\{b, c\}$, $\{b, d\}$, $\{c, d\}$, $\{a, b, c\}$, $\{a, b, d\}$, $\{a, c, d\}$, $\{b, c, d\}$

Q1.24. Show that the number of proper subsets of $S = \{a_1, a_2, \ldots, a_n\}$ is $2^n - 1$.

A1.24. The number of subsets of S is counted by the number of functions from S to $\{0, 1\}$, which is the set 2^S, whose cardinality is $2^{|S|} = 2^n$. Minus the set S itself, we have $2^n - 1$.

Q1.25. Using the sets of Problem 1.2, verify

(a) $(A \cup B) \cup C = A \cup (B \cup C)$

(b) $(A \cap B) \cap C = A \cap (B \cap C)$

(c) $(A \cup B) \cap C \neq A \cup (B \cap C)$

A1.25.

(a)

$$\begin{aligned}(A \cup B) \cup C &= \{a, b, c, d, g\} \cup \{c, g, m, n, p\} \\ &= \{a, b, c, g, m, n, p\} \\ &= \{a, b, c, d\} \cup \{a, c, g, m, n, p\} \\ &= A \cup (B \cup C)\end{aligned}$$

(b) $(A \cap B) \cap C = A \cap (B \cap C)$

(c) $(A \cup B) \cap C \neq A \cup (B \cap C)$

Q1.26.

A1.26.

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 ϕ 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 ϕ happens to also be a bijection of sets, then ϕ 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

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

Let $[G : H]$ denote the number of cosets of H there are in G.

THEOREM XVII. (Lagrange's Theorem) $|G| = [G : H]|H|$

THEOREM XVIII. If G is a finite group of order n, then the order of any element $a \in G$ is a divisor of n.

THEOREM XIX. Every group of prime order is cyclic.

9.9 Normal subgroups

DEFINITION 9.10: A subgroup H of a group G is called a *normal subgroup* of G if $gH = Hg$ for every $g \in G$.

THEOREM XX.

EXAMPLE 2

THEOREM XXI. If $\phi : G \to H$ is a homomorphism, then the inverse image of 1_H under ϕ is a normal subgroup of G.

9.10 Quotient groups

THEOREM XXII. If G has order n and H, a subgroup of G, has order m, then the quotient group G/H has order n/m

THEOREM XXIII. If H is a normal subgroup of G, then the map $g \to Hg$ is a homomorphism from G to G/H.

THEOREM XXIV. Any quotient of a cyclic group is cyclic.

THEOREM XXV. If H is a normal subgroup of G and H is also a subgroup of a subgroup K of G, then H is also a normal subgroup of K.

9.11 Product of subgroups

THEOREM XXVI. If H and K are normal subgroups of G, then HK is a normal subgroup of G.

9.12 Composition series

DEFINITION 9.11: A normal subgroup H of G is called *maximal* if there is no other proper normal subgroup K of G which contains H as a proper subgroup.

DEFINITION 9.12: For any group G a sequence of its subgroups

$$G, H, J, K, \ldots, \nVdash$$

is a *composition series* for G if each group is a maximal normal subgroup of the previous group. Then the groups $G/H, H/J, J/K, \ldots$ are called the *quotient groups of the composition series*

THEOREM XXVII. Every finite group has at least one composition series.

THEOREM XXVIII. (The Jordan-Hölder Theorem) All the composition series of a finite group have the same length. Moreover, their corresponding quotient groups are isomorphic.

THEOREM XXIX.

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

×	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 $\{\mathbf{u} = (1), \rho, \rho^2, \rho^3, \sigma^2, \tau^2, b = (13), e = (24)\}$ of S_4 is a group (see the operation table below), called the *octic group of a square* or the dihedral group. We shall now show how this permutation group may be obtained using properties of symmetry of a square.

A9.9.

Q9.10. A permutation group on n symbols is called *regular* if each of its elements except the identity moves all n symbols. Find the regular permutation groups on four symbols.

A9.10.

Q9.11. Prove: The mapping $\mathbb{Z} \to \mathbb{Z}_n : m \to [m]$ is a homomorphism of the additive group $\mathbb{Z}$ onto the additive group $\mathbb{Z}_n$ of integers modulo n.

A9.11.

Q9.12. In a homomorphism between two groups $\mathcal{G}$ and $\mathcal{G}'$, their identity elements correspond, and if $x \in \mathcal{G}$ and $x' in \mathcal{G}'$ correspond so also do their inverses.

A9.12. Let 1 be the identity of $\mathcal{G}$ and $1'$ the identity of $\mathcal{G}'$. Let ϕ be a homomorphism from $\mathcal{G}$ to $\mathcal{G}'$. Let x be any non-identity element of $\mathcal{G}$. Then $1' \square \phi(x) = \phi(x) = \phi(1 \circ x) = \phi(1) \square \phi(x)$. Then $\phi(1) = 1'$.

Q9.13. Prove: every cyclic group of infinite order is isomorphic to the additive group $\mathbb{Z}$.

A9.13. Let $\mathcal{G}$ be an infinite cyclic group generated by a, and consider the homomorphism $\mathbb{Z} \to \mathcal{G}$ defined by $n \to a^n$. This is a homomorphism because $a^{s+t} = a^s a^t$. It is onto, and moreover, is into because it has a trivial kernel. If it didn't, then it means that there existed m such that $a^m = 1$, which would have implied $\mathcal{G}$ is not finite, a contradiction. Hence the map is an isomorphism.

Q9.14. Prove: Every finite group of order n is isomorphic to a permutation group on n symbols.

A9.14. Consider a group's action on itself by left translation yadda yadda.

Q9.15. Prove: The kernel of a homomorphism is a normal subgroup.

A9.15. Let ϕ be a homomorphism from G to H. Let K be the kernel of ϕ. Let $a, b \in K$. First, we show that $K < G$.

Let $a, b \in K$. Then $\phi(ab) = \phi(a)\phi(b) = 1_H 1_H = 1_H$, so $ab \in K$. Also, $\phi(a^{-1}) = \phi(a)^{-1} = 1_H^{-1} = 1_H$, so $a^{-1} \in K$.

Hence $K < G$. Next we show that K is normal. Let $g \in G$ and $k \in K$. Then $\phi(g^{-1}kg) = \phi(g)^{-1} 1_H \phi(g) = \phi(g)^{-1}\phi(g) = 1_H$, hence $g^{-1}kg \in K$. Then $K \triangleleft G$

Q9.16. Prove: The product of cosets

$$(Ha)(Hb) = \{(h_1 a)(h_2 b) : h_1, h_2 \in H\}$$

where $H \triangleleft G$ is well defined.

A9.16. $(Ha)(Hb) = H(aHb) = (HH)(ab) = H(ab)$

Q9.17. Prove: Any quotient group of a cyclic group is cyclic

A9.17. Let G be cyclic, and generated by a, and let $H \triangleleft G$. Since G is abelian, $(Ha)^m = H^m a^m = Ha^m$. Since every coset of H in G is of the of the form Ha^m, we have proven that Ha generates G/H.

Q9.18. Prove: Every finite group has at least one composition series.

A9.18. Lemma: If a finite group has proper normal subgroups, it contains a maximal normal subgroup. Proof: Take the product of proper normal subgroups.

Then just use induction.

Q9.19.

A9.19.

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