# Advanced Modern Algebra second edition

Selected Solutions
Chapter 1: Groups I

January 11, 2024

## 1.1. Classical Formulas

**Exercise 1.1.** Given $M, N \in \mathbb{C}$, prove that there exists $g, h \in \mathbb{C}$ with $g + h = M$ and $gh = N$.

*Proof.* Consider the quadratic equation $x^2 - Mx + N = 0$ and apply the quadratic formula, we have two roots $r_1 = \frac{-M+\sqrt{M^2-4N}}{2}$ and $r_2 = \frac{-M-\sqrt{M^2-4N}}{2}$. Notice that $r_1 + r_2 = -M$ and $r_1 r_2 = N$. Then we see that $-r_1, -r_2 \in \mathbb{C}$ that satisfies the relation. □

**Exercise 1.3.** (i) Find the complex roots of $f(x) = x^3 - 3x + 1$.

(ii) Find the complex roots of $f(x) = x^4 - 2x^2 + 8x - 3$.

**Exercise 1.4.** Show that the quadratic formula does not hold for $f(x) = ax^2 + bx + c$ if we view the coefficients $a, b, c$ as lying in the integers mod 2.

*Proof.* Take $f(x) = x^2 + x + 1$, applying the quadratic formula, we have $r_1 = \frac{-1+\sqrt{1-4}}{2} = \frac{1+1}{2} = 1 \neq 0$ and $r_2 = \frac{-1-\sqrt{1-4}}{2} = \frac{1-1}{2} = 1 \neq 0$. □

## 1.2. Permutations

**Exercise 1.5.** Give an example of functions $f : X \to Y$ and $g : Y \to X$ such that $gf = 1_X$ and $fg \neq 1_Y$.

*Proof.* Consider $f : \mathbb{Z} \to \mathbb{Z}, g : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = -x, g(x) = |x|$. Then we see that $gf(x) = |-x| = x$, $\forall x \in \mathbb{Z}$ while $fg(1) = -|1| = -1$. □

**Exercise 1.6.** Prove that the composition of functions is associative: if $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W$, then

$$h(gf) = (hg)f.$$

*Proof.* $h(gf)(x) = h(g(f(x)) = (hg)f(x)$ □

**Exercise 1.7.** Prove that the composite of two injections is an injection, and that the composite of two surjections is a surjection. Conclude that the composite of two bijections is a bijection.

*Proof.* Injection: Suppose we have $f : X \to Y$, $g : Y \to Z$ both injections. Then we see that $\forall a_1, a_2 \in X$, $a_1 = a_2 \implies f(a_1) = f(a_2) \implies g(f(a_1)) = g(f(a_2))$. Hence the composition of two injections is an injection.
Surjection: Suppose we have $f : X \to Y$, $g : Y \to Z$ both surjections. Then we see that $\forall c \in Z, \exists b \in Y$ s.t. $g(b) = c$. Also, since $f$ is surjective, there is $a \in X$ s.t. $f(a) = b$. Hence there is $a \in X$ with $g(f(a)) = c$ for all $c \in Z$.
Bijection: Since bijections are injective and surjective at the same time, compositions of two bijections must also be both injective and surjective at the same time. □

**Exercise 1.8 (Pigeonhole Principle).** (i) Let $f : X \to X$ be a function, where $X$ is a finite set. Prove equavalence of the following statements.

(a) $f$ is an injection.

(b) $f$ is a bijection.

(c) $f$ is a surjection.

(ii) Prove that no two of the statements in (i) are equivalent when $X$ is an infinite set.

(iii) Suppose there are 501 pigeons, each sitting in some pigeonhole. If there are only 500 pifeonholes, prove that there is a hole containing more than one pigeon.

*Proof.* (i) Since bijective iff surjective and injective, we only need to proof $(a)$ iff $(c)$.
Suppose $f$ is injective, then no two elements in $X$ are mapped to the same element, hence $|X| = |f(X)|$ or equavalently, $f$ is surjective.

(ii) Consider $f : \mathbb{N} \to \mathbb{N}$ where $f(x) = x + 1$. We see that $f$ is an injection, but not surjection, since 1 does not have a preimage. This implies that injective cannot be equavalent to surjection, and hence the three statements are not equal to each other.

(iii) We prove the contrapositive, if each of the 500 pigeonholes contain only one pigeon, then there has to be exactly 500 pigeons. This is obvious by (i) as we have 500 pigeons to map to 500 pigeionholes, then surjectivity implies bijectivity and hence there are 500 pigeions.

□

**Exercise 1.9.** Let $Y$ be a subset of a finite set $X$, and let $f : Y \to X$ be an injection. Prove that there is a permutation $\alpha \in S_X$ with $\alpha|Y = f$.

**Exercise 1.10.** Find $\text{sgn}(\alpha)$ and $\alpha^{-1}$, where

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

**Exercise 1.11.** If $\alpha \in S_n$, prove that $\text{sgn}(\alpha^{-1}) = \text{sgn}(\alpha)$.

**Exercise 1.12.** If $1 \leq r \leq n$, show that there are

$$\frac{1}{r}[n(n-1)...(n-r+1)]$$

$r$-cycles in $S_n$.

**Hint .** There are exactly $r$ cycle notations for any $r-$cycle.

**Exercise 1.13.** (i) If $\alpha$ is an $r-$cycle, show that $\alpha^r = (1)$.

**Hint .** If $\alpha = (i_0...i_{r-1})$, show that $\alpha^k(i_0) = i_j$, where $k = qr + j$ and $0 \leq j < r$.

(ii) If $\alpha$ is an $r-$cycle, show taht $r$ is the smallerst positive integer $k$ such that $\alpha^k = (1)$.

**Exercise 1.14.** Show that an $r-$cycle is an even permutation if and only if $r$ is odd.

**Exercise 1.15.** (i) Let $\alpha = \beta\delta$ be a factorization of a permutation $\alpha$ into disjoint permutations. If $\beta$ moves $i$, prove that $\alpha^k(i) = \beta^k(i)$ for all $k \geq 1$.

(ii) Let $\beta$ and $\gamma$ be cucles both of which move $i$. If $\beta^k(i) = \gamma^k(i)$ for all $k \geq 1$, prove that $\beta = \gamma$.

**Exercise 1.16.** Given $X = 1, 2, ..., n$, let us call a permutation $\tau$ of $X$ an ***adjacency*** if it is a transposition of the form $(i\ i+1)$ for $i < n$.

(i) Prove that every permutation in $S_n$, for $n \geq 2$, is a product of adjacencies.

(ii) If $i < j$, prove that $(i\ j)$ is a product of an odd number of adjacencies.

**Hint .** Use induction on $j - i$.

**Exercise 1.17.** (i) Prove, for $n \geq 2$, that every $\alpha \in S_n$ is a product of transpositions each of whose factors moves $n$.

**Hint .** If $i < j < n$, then $(j\ n)(i\ j)(j\ n) = (i\ n)$, by Lemma 1.7, so that $(i\ j) = (j\ n)(i\ n)(j\ n)$.

(ii) Why doesn't part (i) prove that a 15-puzzle with even starting position $\alpha$ which fixes $\square$ can be solved?

**Exercise 1.18.** Define $f : 0, 1, 2, ..., 10 \to 0, 1, 2, ..., 10$ by

$$f(n) = \text{the remainder after dividing } 4n^2 - 3n^7 \text{ by } 11.$$

(i) Show that $f$ is a permutation.

(ii) Compute the parity of $f$.

(iii) Compute the inverse of $f$.

**Exercise 1.19.** If $\alpha$ is an $r-$cucle and $1 < k < r$, is $\alpha^k$ an $r-$cycle?

**Exercise 1.20.** (i) Prove that if $\alpha$ and $\beta$ are (not necessarily disjoint) permutations that commute, then $(\alpha\beta)^k = \alpha^k\beta^k$ for all $k \geq 1$.

**Hint .** First show that $\beta\alpha^k = \alpha^k\beta$ by induction on $k$.

(ii) Given an example of two permutations $\alpha$ and $\beta$ for which $(\alpha\beta)^2 \neq \alpha^2\beta^2$.

**Exercise 1.21.** (i) Prove, for all $i$, that $\alpha \in S_n$ moves $i$ if and only if $\alpha^{-1}$ moves $i$.

(ii) Prove that if $\alpha, \beta \in S_n$ are disjoint and if $\alpha\beta = (1)$, then $\alpha = (1)$ and $\beta = (1)$.

**Exercise 1.22.** Prove that the number of even permutations in $S_n$ is $\frac{1}{2}n!$.

**Hint .** Let $\tau = (1\,2)$, and define $f : A_n \to O_n$, where $A_n$ is the set of all even permutations in $S_n$ and $O_n$ is the set of all odd permutations, by $f : \alpha \to \tau\alpha$. Show that $f$ is a bijection, so that $|A_n| = |O_n|$ and, hence, $|A_n = \frac{1}{2}n!$.

**Exercise 1.23.** (i) How many permutations in $S_5$ commute with $\alpha = (1\,2\,3)$, and how many $textifeven$ permutations in $S_5$ commute with $\alpha$?

**Hint .** Of the six permutations in $S_5$ commuting with $\alpha$, only three are even.

(ii) Same question for $(1\,2)(3\,4)$.

**Hint .** Of the eight permutations in $S_4$ commuting with $(1\,2)(3\,4)$, only four are even.

**Exercise 1.24.** Given an example of $\alpha, \beta, \gamma \in S_5$, with $\alpha \neq (1)$, such that $\alpha\beta = \beta\alpha, \alpha\gamma = \gamma\alpha$, and $\beta\gamma \neq \gamma\beta$.

**Exercise 1.25.** If $n \geq 3$, prove that if $\alpha \in S_n$ commutes with every $\beta \in S_n$, thwn $\alpha = (1)$.

**Exercise 1.26.** If $\alpha = \beta_1 ... \beta_m$ is a product of disjoint cycles and $\delta$ is disjoint from $\alpha$, show that $\beta_1^{e_1} ... \beta_m^{e_m}\delta$ commutes with $\alpha$, where $e_j \geq 0$ for all $j$.

## 1.4. Lagrange's Theorem

**Exercise 1.38.** Let $H$ be a subgroup of a group $G$.

(i) Prove that right cosets $Ha$ and $Hb$ are equal if and only if $ab^{-1} \in H$.

(ii) Prove that the relation $a \equiv b$ if $ab^{-1} \in H$ is an equivalence relation on $G$ whose equivalence classes are the right cosets of $H$.

*Proof.* $\Longrightarrow$ : $Ha = Hb$ implies that Given $a, b \in G$, $\forall h \in H, \exists h' \in H$ s.t. $ha = h'b$. This implies that $ab^{-1} = h^{-1}h' \in H$.

$\Longleftarrow$ : $ab^{-1} \in H$ implies that $\forall h \in H$ there is $hab^{-1} \in H$, which implies that there is $h' \in H$ s.t. $hab^{-1} = h'$, which is equavalently $ha = h'b$, hence $Ha = Hb$.

□

**Exercise 1.39.** (i) Define the **special linear group** by

$$\mathrm{SL}(2, \mathbb{R}) = \{A \in \mathrm{GL}(2, \mathbb{R}) : \det(A) = 1\}.$$

Prove that SL(2, $\mathbb{R}$) is a subgroup of GL(2, $\mathbb{R}$).

(i) Prove that SL(2, $\mathbb{Q}$) is a subgroup of GL(2, $\mathbb{R}$).

*Proof.* (i): We can easliy check that the two by two identity $I \in$ SL(2, $\mathbb{R}$)), product of matrices with determinant 1 remains determinant 1, and that SL(2, $\mathbb{R}$) is subset of invertible matrices. (2): Similar, noticing that $\mathbb{Q}$ is subgroup of $\mathbb{R}$. □

**Exercise 1.40.** (i) Give an example of two subgroups $H$ and $K$ of a group $G$ whose union $U \cup K$ is not a subgroup of G.

**Hint .** Let $G$ be the four-group $\mathbf{V}$.

(ii) Prove that the union $H \cup K$ of two subgroups is itself a subgroup if and only if $H$ is a subset of $K$ or $K$ is a subset of $H$.

*Proof.* (i) Easy to verify that $H = \{(1), (12)(34)\}$ and $K = \{(1), (13)(24)\}$ are subgroups of $D_4$ but that $(12)(34)(13)(24) = (14)(23)$ is not in $H \cup K$.

(ii) $\Longleftarrow$ is trivial, so we prove $\Longrightarrow$. Consider proving the contrapositive statement, if $K \nsubseteq H$ and $H \nsubseteq K$, $\exists k \in K, h \in H$ s.t. $k \notin H, h \notin K$, then for any $h \in H$, $hk \notin H$ since if $hk = h' \in H$, then $k = h^{-1}h' \in H$, contradicts to assumption, similarly $hk \notin K$. Hence $hk \notin H \cup K$ and $H \cup K$ cannot be a subgroup.

□

**Exercise 1.41.** Let $G$ be a finite group with subgroups $H$ and $K$. If $H \subseteq K \subseteq G$, prove that

$$[G : H] = [G : K][K : H].$$

*Proof.* $[G : K][K : H] = \frac{|G|}{|K|}\frac{|K|}{|H|} = \frac{|G|}{|H|} = [G : H]$ □

**Exercise 1.42.** If $H$ and $K$ are subgroups of a group $G$ and $|H|$ and $|K|$ are relatively prime, prove that $H \cap K = \{1\}$.

**Hint .** If $x \in H \cap K$, then $x^{|H|} = 1 = x^{|K|}$.

*Proof.* Following hint, without loss of generality assume that $|H| \leq |K|$. Since $|H|$ and $|K|$ are co-prime, we know there is no $d < |H|$ s.t. $x^d = 1$ since that would imply $d \mid |H|$ and $d \mid |K|$. Then $|H|$ must be order of $x$ and hence divides $|K|$, contradiction. □

**Exercise 1.43.** Let $G$ be a group of order 4. Prove that either $G$ is cyclic or $x^2 = 1$ for every $x \in G$. Conclude, using Exercise 1.35 on page 27, that $G$ must be abelian.

*Proof.* We know $\mathbb{Z}/4\mathbb{Z}$ is cyclic group of order 4, so we know the exsistance. We only need to show that if $G$ is not cyclic, then $x^2 = 1$ for all $x \in G$. Assuming other wise, there exists group $G$ of order 4 and $x \in G$ with $x^2 \neq 1$, since order of $x$ divides 4, we have either $x = 1$ or $x^4 = 1$, either case $x^4 = 1$ and implies that $G$ is cyclic.

If $G$ cyclic, then $G$ is abelian as $a^x a^y = a^(x + y) = a^y a^x \forall x \in G$ for any group $G$. Since Exericise 1.35 implies that $G$ is abelian if $x^2 = 1$ for all $x \in G$, all group of order 4 are abelian. □

**Exercise 1.44.** If $H$ is a subgroup of a group $G$, prove that the number of left cosets of $H$ in $G$ is equal to the number of right cosets of $H$ in $G$.

**Hint .** The function $\varphi : aH \mapsto Ha^{-1}$ is a bijection from the family of all left cosets of $H$ to the family of all right cosets of $H$.

*Proof.* First show that $\varphi$ is well defined: $aH = bH \implies \varphi(aH) = \varphi(bH)$. $aH = bH \iff a^{-1}b \in H$ $Ha^{-1} = Hb^{-1} \iff a^{-1}(b^{-1})^{-1} \in H$ by Exercise 1.38 we know that $a^{-1}(b^{-1})^{-1} = a^{-1}b \in H$ hence $aH = bH \implies \varphi(aH) = \varphi(bH)$.

Injection: If $\exists a, b \in G$ s.t. $\varphi(aH) = \varphi(bH)$, then $Ha^{-1} = Hb^{-1}$ so $existsh \in H, a^{-1} = hb^{-1}$ Hence $h = a^{-1}b$ and $h^{-1} = b^{-1}a \in H$ since $H$ is subgroup. This is equavlently $aH = bH$, proving injectivity.

Surjection: Let $Ha$ be a coset of $H$, since $a = (a^{-1})^{-1}$, we know that $Ha = \varphi(a^{-1}H)$ and hence surjective.

□

**Exercise 1.45.** If $p$ is an odd prime and $a_1, ..., a_{p-1}$ is a permutation of $\{1, 2, ..., p-1\}$, prove that there exists $i \neq j$ with $ia_i \equiv ja_j \mod p$.

**Hint .** Use Wilson's Theorem.

*Proof.* □

## 1.5. Homomorphisms

**Exercise 1.46.** Show that if there is a bijection $f : X \to Y$ (that is, if $X$ and $Y$ have the same number of elements), then there is an isomorphism $\varphi : S_X \to S_Y$.

**Hint .** If $\alpha \in S_X$, define $\varphi(\alpha) = faf^{-1}$. In particular, show that if $|X| = 3$, then $\varphi$ takes a cycle involving symbols 1, 2, 3 into a cycle involving a,b,c as in Example 1.57.

**Exercise 1.47.** (i) Show that the composite of Homomorphisms is it self a Homomorphism.

(ii) Show that the inverse of an isomorphism is an isomorphism.

(iii) Show that two groups that are isomorphic to a third groupd are isomorphic to each other.

(iv) Prove that iso,orphisms is an equavalence relation on any set of groups.

**Exercise 1.48.** Prove that a group G is abelian if and only if the function $f : G \to G$, given by $f(a) = a^{-1}$, is a homomorphism.

**Exercise 1.49.** This exercise gives some invariants of a group $G$. Let $f : G \to H$ be an isomorphism.

(i) Prove that if $a \in G$ has infinite orderm then so does f(a), and if $a$ has finiteg order $n$, then so does $f(a)$. Concluded that if $G$ has an element of some order $n$ and $H$ does not, then $G \ncong H$.

(ii) Prove that if $G \ncong G$, then, for every divisor $d$ of $|G|$, bnoth $G$ and $H$ have the same number of elements of order $d$.

(iii) If $a \in G$, then its **conjugacy class** is $\{gag^{-1} : g \in G\}$. If $G$ and $H$ are isomoirphic groups, prove that they have the same number of conjugacy classes. Indeed, if $G$ has exactly $c$ conjugacy classes of size $s$, then so does $H$.

**Exercise P.** rove that $A_4$ and $D_{12}$ are nonisomorphic groups of order 12.