Selected Exercises From Dummit And Foote

Shannon Heylmun

November 25, 2015

Contents

Chapter 0

Preliminaries

0.1 The Basics

In 1 through 4, let $\mathcal{A}$ be the set of 2×2 matrices with real number entries. Let

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and let $\mathcal{B} = \{X \in \mathcal{A} | MX = XM\}$

1. Determine which of the following elements of $\mathcal{A}$ lie in $\mathcal{B}$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

2. Prove that if $P, Q \in \mathcal{B}$, then $P + Q \in \mathcal{B}$.

3. Prove that if $P, Q \in \mathcal{B}$, then $P \cdot Q \in \mathcal{B}$.

4. Find conditions on p, q, r, s which determine precisely when

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{B}$$

5. Determine whether the following functions f are well defined:

   (a) $f : \mathbb{Q} \to \mathbb{Z}$ defined by $f(a/b) = a$.

   (b) $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(a/b) = a^2/b^2$.

6. Determine whether the function $f : \mathbb{R}^+ \to \mathbb{Z}$ defined by mapping a real number r to the first digit to the right of the decimal point in a decimal expansion of r is well defined.

7. Let $f : A \to B$ be a surjective map of sets. Prove the relation $a \sim b$ if and only if $f(a) = f(b)$ is an equivalence relation whose equivalence classes are the fibers of f.

0.2 Properties of the Integers

1. For each of the following pairs of integers a and b, determine the GCD, LCM, and write the GCD in the form $ax + by$ for some integers x and y.

   (a) $a = 792, b = 275$

   $$\begin{aligned} 792 &= (3)275 + 11 \\ 275 &= (25)11 + 0 \\ &\Rightarrow GCD(792, 275) = 11 \end{aligned}$$

   Since $dl = ab$ where d is the GCD of a and b and l is the LCM, we see that $11l = 275 \cdot 792$. Solving for l, we find that the LCM of 275 and 792 is 19800.
   We can see that $11 = 792(1) - 275(3)$.

   (b) $a = 1761, b = 1567$

   $$\begin{aligned} 1761 &= (1)1567 + 194 \\ 1567 &= (8)194 + 15 \\ 194 &= (12)15 + 14 \\ 15 &= 14 + 1 \\ &\Rightarrow GCD(1761, 1567) = 1 \end{aligned}$$

   Since a and b are relatively prime, their LCM is the product $1567 \cdot 1761 = 2,759,487$. The GCD can be written as the linear combination $1 = 118(1567) - 105(1761)$.

2. Prove that if the integer k divides the integers a and b, then k divides $as + bt$ for every pair of integers s and t.

   Proof. Let $k, a, b \in \mathbb{Z}$ such that $k|a$ and $k|b$. This means that $a = km$ and $b = kn$ for some integers m and n. Let $s, t \in \mathbb{Z}$. Then we see that

   $$\begin{aligned} as + bt &= kms + knt \\ &= k(ms + nt) \end{aligned}$$

   Since $k|k(ms + nt)$, the claim is proven. □

3. Prove that if n is composite, then there are integers a and b such that n divides ab but n does not divide a nor b.

   Proof. Let n be composite. Then n may be written as $a \cdot b$ where $1 < a, b < n$. Since n divides itself, $n|a \cdot b$; however, since $a, b < n$, it is impossible for n to divide a or b. □

4. Let a, b and N be fixed integers with $a, b \neq 0$ and let $d = (a, b)$. Suppose x_0 and y_0 are particular solutions to $ax + by = N$. Prove that for any integer t, the integers

   $$x = x_0 + \frac{b}{d}t \text{ and } y = y_0 - \frac{a}{d}t$$

   are also solutions to $ax + by = N$.

Proof. Let $a, b, N \in \mathbb{Z}$ with $a, b \neq 0$, and let $d = \gcd(a, b)$. Let x_0 and y_0 be solutions to $ax + by = N$, and let t be an arbitrary real number.

$$\begin{aligned} & a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) \\ =& ax_0 + \frac{ab}{d}t + by_0 - \frac{ba}{d}t \\ =& ax_0 + by_0 = N \end{aligned}$$

This proves the claim. □

5. Determine the value of $\psi(n)$ for each integer $n \leq 30$ where ψ denotes the Euler ψ-function.

6. Prove the Well Ordering Property of $\mathbb{Z}$ by induction and prove the minimal element is unique.

7. If p is prime, prove that there do not exist nonzero integers a and b such that $a^2 = pb^2$ (i.e., $\sqrt{p} \notin \mathbb{Q}$).

   Proof. Let p be prime. Suppose toward a contradiction that $a, b \in \mathbb{Z}$ with $a \neq b$, $a, b \neq 1$ such that $a^2 = pb^2$. This implies that

   $$p = \frac{a^2}{b^2}$$

   Note that $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$ (by the fundamental theorem of arithmetic). We can then see that $a^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} ... p_n^{2\alpha_n}$ has an even number of prime factors. The same can be said of b.

   Since the qotient a^2/b^2 is prime, every prime factor of b^2 must be a factor of a^2.

   There are an even number of such factors, and since $a \neq b$ and $a^2/b^2 > 1$ there must be a greater (even) number of prime factors of a^2. This implies that the prime factorization of a^2 contains at least two factors, so p cannot be prime. This contradiction proves the claim. □

8. Let p be prime, $n \in \mathbb{Z}^+$. Find a formula for the largest power of p which divides $n!$.

9. Write a computer program to determine (a, b) and to express (a, b) in the form $ax + by$ for some integers x and y.

10. Prove that for any given positive integer N, there exist only finitely many integers n with $\psi(n) = N$. Conclude in particular that $\psi(n)$ tends to infinity as n tends to infinity.

11. Prove that if d divides n then $\psi(d)$ divides $\psi(n)$.

    Proof. Let $n, d \in \mathbb{Z}$ such that $d|n$. We then see that every prime factor d_i of d also divides n, and is therefore a prime factor of n. Suppose that $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$. We then know that

    $$\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) ... p_m^{\alpha_m - 1}(p_m - 1)$$

    Since $d|n$, $d = d_1^{\delta_1} d_2^{\delta_2} ... d_n^{\delta_n}$ where $d_i \in \{p_i\}$. We also know that

    $$\phi(d) = d_1^{\delta_1 - 1}(d_1 - 1) d_2^{\delta_2 - 1}(d_2 - 1) ... d_m^{\delta_m - 1}(d_m - 1)$$

    Since every d_i is an element of $\{p_j | 1 \leq j \leq m\}$, and we may then infer that each $d_i - 1$ is an element of $\{p_j - 1 | 1 \leq j \leq m\}$, we see that every factor of $\phi(d)$ is a factor of $\phi(n)$, and the claim is shown. □

0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Mod n

1. Write all the elements of the residue classes of $\mathbb{Z}/18\mathbb{Z}$.

   Solution 1.

$$\begin{aligned}
\overline{0} &= \{..., -18, 0, 18, ...\} \\
\overline{1} &= \{..., -17, 1, 19, ...\} \\
\overline{2} &= \{..., -16, 2, 20, ...\} \\
\overline{3} &= \{..., -15, 3, 21, ...\} \\
\overline{4} &= \{..., -14, 4, 22, ...\} \\
\overline{5} &= \{..., -13, 5, 23, ...\} \\
\overline{6} &= \{..., -12, 6, 24, ...\} \\
\overline{7} &= \{..., -11, 7, 25, ...\} \\
\overline{8} &= \{..., -10, 8, 26, ...\} \\
\overline{9} &= \{..., -9, 9, 27, ...\} \\
\overline{10} &= \{..., -8, 10, 28, ...\} \\
\overline{11} &= \{..., -7, 11, 29, ...\} \\
\overline{12} &= \{..., -6, 12, 30, ...\} \\
\overline{13} &= \{..., -5, 13, 31, ...\} \\
\overline{14} &= \{..., -4, 14, 32, ...\} \\
\overline{15} &= \{..., -3, 15, 33, ...\} \\
\overline{16} &= \{..., -2, 16, 34, ...\} \\
\overline{17} &= \{..., -1, 17, 35, ...\}
\end{aligned}$$

2. Prove that the distinct equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ are precisely $\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}$ (use the Division Algorithm).

3. Prove that if $a = a_n 10^n + a_{n-1}10^{n-1} + ... + a_1 10 + a_0$ is any positive integer, then $a \equiv a_n + a_{n-1} + ... + a_1 + a_0 \pmod 9$.

   Proof. Let $a = a_n 10^n + a_{n-1}10^{n-1} + ... + a_1 10^1 + a_0$. We will begin by showing that

$$10^n \equiv 1 \pmod 9$$

   for any $n \in \mathbb{Z}^+$ by induction.

   Base case: $10^1 \equiv 1 \pmod 9$ is clear.

   Induction step: Assume that $10^n \equiv 1 \pmod 9$. Then

$$10^{n+1} = 10 \cdot 10^n \equiv 1 \cdot 1 \pmod 9 \equiv 1 \pmod 9$$

   We can therefore use the fact that to conclude that $a \equiv a_n + a_{n-1} + ... + a_1 + a_0 \pmod 9$. □

4. Compute the remainder when 37^{100} is divided by 29.

Solution 2.

$$\begin{aligned}
37^{100} &\equiv & 8^{100} &\pmod 9\\
&\equiv & 8^{100} &\pmod 9\\
&\equiv & (2^5)^{60} &\pmod 9\\
&\equiv & 32^{60} &\pmod 9\\
&\equiv & (3^3)^{20} &\pmod 9\\
&\equiv & (-2)^{20} &\pmod 9\\
&\equiv & 2^{20} &\pmod 9\\
&\equiv & (2^5)^{4} &\pmod 9\\
&\equiv & 32^{4} &\pmod 9\\
&\equiv & 3^3\cdot 3 &\pmod 9\\
&\equiv & -6 &\pmod 9\\
&\equiv & 23 &\pmod 9
\end{aligned}$$

5. Compute the last two digits of 9^{1500}.

Solution 3.

$$\begin{aligned}
9^{1500} &= & (9^3)^{500}\\
&= & 729^{500}\\
&\equiv & 29^{500} &\pmod{100}\\
&\equiv & 41^{250} &\pmod{100}\\
&\equiv & 81^{500} &\pmod{100}\\
&\equiv & 9^{125}\cdot 9^{125} &\pmod{100}\\
&\equiv & 49^{25}\cdot 49^{25} &\pmod{100}\\
&\equiv & 1^{25} &\pmod{100}\\
&\equiv & 1 &\pmod{100}
\end{aligned}$$

6. Prove that the squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\overline{0}$ and $\overline{1}$.

Proof. Let $\overline{a} \in \mathbb{Z}/4\mathbb{Z}$.

(a) If $\overline{a} = \overline{0}$

(b) If $\overline{a} = \overline{2}$

(c) If $\overline{a} = \overline{0}$

(d) If $\overline{a} = \overline{0}$

$\square$

7. Prove for any integers a and b that $a^2 + b^2$ never leaves a remainder of 3 when divided by 4.

   Proof. Let $a, b \in \mathbb{Z}$. Consider $a^2 + b^2$. Since $a^2 \equiv \overline{0}$ or $\overline{1} \pmod 4$ always, and the same holds for b^2, we have $a^2 + b^2 \equiv \overline{0}, \overline{1}$, or $\overline{2} \pmod 4$ always. □

8. Prove that the equation $a^2 + b^2 = 3c^2$ has no solutions in nonzero integers a, b, and c.

   Proof. By the previous exercise, $a^2 + b^2 \equiv \overline{0}, \overline{1}$, or $\overline{2} \pmod 4$ for any integers a and b. By the penultimate exercise, $c^2 \equiv \overline{0}$ or $\overline{1} \pmod 4$.

   □

9. Prove that the square of any odd integer always leaves a rremainder of 1 when divided by 8.

   Proof. Let $n \in \mathbb{Z}$ be odd. Then $n = 2 \cdot m + 1$ for some $m \in \mathbb{Z}$. We can then consider n^2

$$\begin{aligned} n^2 =& (2m+1)^2 \\ =& 4m^2 + 4m + 1 \\ =& 4m(m+1) + 1 \end{aligned}$$

   If m is even, then $8|4m$; otherwise, $8(m+1)$. This proves that $4m(m+1) \equiv 0 \pmod 8$, so $n = 4m(m+1) + 1 \equiv 1 \pmod 8$. □

10. Prove that the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\psi(n)$.

11. Prove that if $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

12. Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if a and n are not relatively prime, there exists an integer b with $1 \leq b < n$ such that $ab \equiv 0 \pmod n$ and there cannot be an integer c such that $ac \equiv 1 \pmod n$.

    Proof. Let $n \in \mathbb{Z}, n > 1$ and $a \in \mathbb{Z}, 1 \leq a \leq n$. Suppose that $\gcd(a, n) \neq 1$. Then there exists some $m \in \mathbb{Z}^+$ such that $m|a, m|n$ and $1 \leq m \leq a$. Let b be such a number. Then consider $b \cdot a$. Since $b|n$, $b \cdot a \equiv \overline{0} \pmod n$.

    □

13. Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove that if a and n are relatively prime then there is an integer c such that $ac \equiv 1 \pmod n$.

14. Prove that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\overline{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$.

15. For each of the following pairs of integers a and n, show that a is relatively prime to n and determine the multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$.

    (a) $a = 13, n = 20$
    (b) $a = 69, n = 89$
    (c) $a = 1891, n = 3797$
    (d) $a = 6003722857, n = 77695236973$

16. Write a computer program to add and multiply $\pmod n$ for any given n. Outputs should be the least residues of the operations. Include the feature that if $(a, n) = 1$, an integer c between 1 and $n - 1$ such that $\overline{ac} = \overline{1}$ may be printed on request.

Chapter 1

Introduction to Groups

1.1 Basic Axioms and Examples

Let G be a group.

1. Determine which of the following binary operations are associative:

   (a) the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$

   (b) the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$

   (c) the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \dfrac{a+b}{5}$

   (d) the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$

   (e) the operation $\star$ on $\mathbb{Q} - \{0\}$ defined by $a \star b = \dfrac{a}{b}$

2. Decide which of the binary operations in the preceding exercise are commutative.

3. Prove that addition of the residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative. Assume it is well defined.

4. Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative. Assume it is well defined.

5. Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

6. Determine which of the following sets are groups under addition:

   (a) Rational numbers in lowest terms whose denominators are odd.

   (b) Rational numbers in lowest terms whose denominators are even.

   (c) Rational numbers of absolute value less than 1.

   (d) Rational numbers of absolute value greater than or equal to 1 and including 0.

   (e) Rational numbers with denominators equal to 1 or 2.

   (f) Rational numbers with denominators equal to 1, 2, or 3.

7. Let $G = \{x \in \mathbb{R} | 0 \leq x < 1\}$ and for $x, y \in G$, let $x \star y$ be the fractional part of $x + y$. Prove that $\star$ is a well defined binary operation on G and G is an abelian group under $\star$ (called the **real numbers** $\pmod 1$).

8. Let $G = \{z = in\mathbb{C} | z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

   (a) Prove that G is a group under multiplication (called the **group of roots of unity in** $\mathbb{C}$).

   (b) Prove that G is not a group under addition.

9. Let $G = \left\{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Q}\right\}$.
   (a) Prove that G is a group under addition.
   (b) Prove that the nonzero elements of G are a group under multiplication.
10. Prove that a finite group is abelian if and only if its group table is a syymmetric matrix.
11. Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.
12. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^{\times}$: $\overline{1}, \overline{-1}, \overline{5}, \overline{7}, \overline{-7}, \overline{13}$.
13. Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$: $\overline{1}, \overline{2}, \overline{6}, \overline{9}, \overline{10}, \overline{12}, \overline{-1}, \overline{-10}, \overline{-18}$.
14. Find the orders of the following elements of the additive group $(\mathbb{Z}/36\mathbb{Z})^{\times}$: $\overline{1}, \overline{-1}, \overline{5}, \overline{13}, \overline{-13}, \overline{17}$.
15. Prove that $(a_1 a_2 ... a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} ... a_1^{-1}$ for all $a_i \in G$.
16. Let $x \in G$. Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.
17. Let $x \in G$. Prove that if $|x| = n$ for some positive integer n, then $x^{-1} = x^{n-1}$.
18. Let $x, y \in G$. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.
19. Let $x \in G$ and let $a, b \in \mathbb{Z}^+$.
   (a) Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.
   (b) Prove that $(x^a)^{-1} = x^{-a}$.
   (c) Establish part (a) for arbitrary integers a and b.
20. For $x \in G$, show that x and x^{-1} have the same order.
21. Let G be a finite group and let $x \in G$ be of order n. Prove that if n is odd, then $x = (x^2)^k$ for some k.
22. If x and g are elements of G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.
23. Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers s and t, prove that $|x^s| = t$.
24. If a and b are commuting elements of G, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$.
25. Prove that if $x^2 = 1$ for all $x \in G$, then G is abelian.
26. Assume H is a nonempty subset of $(G, \star)$ which is closed under $\star$ and under inverses. Prove that H is a group under $\star$ restricted to H (H is a **subgroup of** G).
27. Prove that if x is an element of the group G, then $\{x^n | n \in \mathbb{Z}\}$ is a subgroup of G (called the **cyclic subgroup of** G **generated by** x).
28. Let $(A, \star)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct procuct. Verify all the group axioms for $A \times B$.

(a) Prove that the associative law holds: for all $(a_i, b_i) \in A \times B, i = 1, 2, 3$,
$(a_1, b_1)[(a_2, b_2)(a_3, b_3)] = [(a_1, b_1)(a_2, b_2)](a_3, b_3))$,

(b) Prove that $(1, 1)$ is the identity of $A \times B$, and

(c) Prove that the inverse (a, b) is (a^{-1}, b^{-1}).

29. Prove that $A \times B$ is an abelian group if and only if A and B are.

30. Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commuted and the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

31. Prove that any finite group G of even order contains an element of order 2.

32. If x is an element of finite order n in G, prove that the elements 1, x, x^2, ..., x^{n-1} are all distinct. Deduce that $|x| < G$.

33. Let x be an element of finite order n in G.

    (a) Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, ..., n - 1$.

    (b) Prove that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-i}$ if and only if $i = k$.

34. If x is an element of infinite order in G, prove that the elements x^n, $n \in \mathbb{Z}$ are all distinct.

35. If x is an element of finite order in G, use the Division Algorithm to show that any integral power of x equals one of the elements in the set of $\{1, x, x^2, ..., x^{n-1}\}$.

36. Assume $G = \{1, a, b, c\}$ is a group of order 4. Assume also that G has no element of order 4. Use the cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.