Solutions to Dummit and Foote's *Abstract Algebra*

Written by
James Ha

Contents

Chapter 0

Preliminaries

0.1 Basics

1. It is less of a pain to figure out the form of all matrices in $\mathcal{B}$ than to multiply all of these matrices by M. Such matrices X satisfy

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix} = \begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

That is to say, $r = 0$ and $p = s$ so the matrices X take the form

$$\begin{pmatrix} s & q \\ 0 & s \end{pmatrix}$$

So, of the matrices shown, the following are elements of $\mathcal{B}$:

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

2. If $P, Q \in \mathcal{B}$, then $(P+Q)M = PM + QM = MP + MQ = M(P+Q)$. Therefore, $P + Q \in \mathcal{B}$.

3. If $P, Q \in \mathcal{B}$, then $PQM = PMQ = MPQ$. Therefore, $PQ \in \mathcal{B}$.

4. See the solution to problem 1 above.

5. (a) This function is not well-defined. For example, $\frac{1}{2}$ may be written $\frac{2}{4}$, $\frac{3}{6}$, etc. So it is ambiguous what the value of $f(1/2)$ should be.

5. (b) This function is well defined, since if $a/b = c/d$ then we have $a^2/b^2 = c^2/d^2$.

6. Although the decimal expansion of many real numbers is unique, there are some real numbers that have two different decimal expansions (e.g., $0.4\bar{9} = 0.5$). Therefore, this function is not well defined.

7. This relation is clearly reflexive since $f(a) = f(a)$ $\forall a \in A$. It is symmetric because if $a \sim b$ then $f(a) = f(b)$, which means $f(b) = f(a)$ and therefore, $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, then $f(a) = f(b)$ and $f(b) = f(c)$. This means that $f(a) = f(c)$ and therefore, $a \sim c$. Thus, the relation is transitive as well, and is an equivalence relation. The equivalence classes are sets of elements in A that map to the same element in B, which are exactly the fibers of f.

0.2 Properties of the Integers

1. (a) Since 13 is prime, their greatest common divisor is 1. Their least common multiple is 260. We may write $2 \cdot 20 - 3 \cdot 13 = 1$

1. (b) Their greatest common divisor is 3. Their least common multiple is 8556. We may write $18 \cdot 372 - 97 \cdot 69 = 3$

1. (c) Their greatest common divisor is 11. Their least common multiple is 19800. We may write $8 \cdot 792 - 23 \cdot 275 = 11$.

1. (d) Their greatest common divisor is 3. Their least common multiple is 21540381. We may write $34426 \cdot 5673 - 17145 \cdot 11391 = 3$.

1. (e) Their greatest common divisor is 1. Their least common multiple is 2759487. We may write $140037984 \cdot 1761 - 157375169 \cdot 1567 = 1$.

1. (f) Their greatest common divisor is 691. Their least common multiple is 44693880. We may write $1479 \cdot 507885 - 12353 \cdot 60808 = 691$.

2. If $k|a$ and $k|b$, then there exist $c, d \in \mathbb{Z}$ such that $a = kc$ and $b = kd$. Then for any integers s, t, we have $as + bt = kcs + kdt = k(cs + dt)$. Since $cs + dt \in \mathbb{Z}$, $k|as + bt$.

3. If n is composite, then there are two integers a, b such that $1 < |a| < n$, $1 < |b| < n$, and $n = ab$. Then $n \nmid a$ and $n \nmid b$, but $n|ab$.

4. Since $d|b$ and $d|a$, clearly $bt/d, at/d \in \mathbb{Z}$ and so are x and y. Then we have

$$ax + by = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + by_0 = N$$

Therefore, for any $t \in \mathbb{Z}$, the given x and y are also solutions to $ax + by = N$.

5. $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(7) = 6$, $\phi(8) = 4$, $\phi(9) = 6$, $\phi(10) = 4$, $\phi(11) = 10$, $\phi(12) = 4$, $\phi(13) = 12$, $\phi(14) = 6$, $\phi(15) = 8$, $\phi(16) = 8$, $\phi(17) = 16$, $\phi(18) = 6$, $\phi(19) = 18$, $\phi(20) = 8$, $\phi(21) = 12$, $\phi(22) = 10$, $\phi(23) = 22$, $\phi(24) = 8$, $\phi(25) = 20$, $\phi(26) = 12$, $\phi(27) = 18$, $\phi(28) = 12$, $\phi(29) = 28$, $\phi(30) = 8$.

6. Assume that there exists a non-empty subset A that has no least element. Then $1 \notin A$ or 1 would be the least element of A. Suppose that all positive integers less than or equal to n are in $\mathbb{Z}^+ \setminus A$. Then $n+1$ cannot be in A either or it would be the least element of A. By induction on n, no positive integer is in A and therefore, $A = \emptyset$. This is a contradiction so every non-empty subset of $\mathbb{Z}^+$ has a least element.

7. Let p be a prime, and suppose there exist nonzero integers a, b such that $a^2 = pb^2$. Assume without loss of generality that $(a,b) = 1$. Note that if $p|a^2$ then $p|a$. Therefore, $\exists c \in \mathbb{Z} \setminus \{0\}$ such that $a = pc$ and $a^2 = pb^2 = p^2c^2$. This, however, implies that $p|(a,b)$, which is a contradiction. Therefore, no such integers a, b exist.

8. The number of integers $\leq n$ that are divisible by p is given by $\left\lfloor \frac{n}{p} \right\rfloor$. Similarly, the number of integers $\leq n$ that are divisible by p^k is given by $\left\lfloor \frac{n}{p^k} \right\rfloor$. These expressions count only a single factor of p from each of these integers. So the expression for the largest power ℓ of p that divides $n!$ is

$$\ell = \sum_k \left\lfloor \frac{n}{p^k} \right\rfloor$$

9. This is trivial and left as an exercise for the reader.

10. Fix N, and note that for any integer n such that $\phi(n) = N$, all of its prime factors must be less than or equal to $N+1$. This must be true, since for any prime $p > N+1$, $\phi(p) > N$, and if p is a prime factor of n, then $\phi(p)|N$, which is clearly absurd. Let $p_1, p_2, \ldots, p_t$ be the primes less than or equal to $N+1$. All numbers n such that $\phi(n) = N$ therefore have a unique prime factorization $n = p_1^{s_1} p_2^{s_2} \ldots p_t^{s_t}$. For $1 \leq i \leq t$, then, $p_i^{s_i - 1}|N$. Let k_i be the largest integer such that $p_i^{k_i}|N$. We require $s_i \leq k_i + 1$ and thus, there are at most $\prod_i (k_i + 1)$ integers n such that $\phi(n) = N$. Since the fiber of ϕ over each positive integer is of finite order, ϕ must tend to infinity as n tends to infinity.

11. Let $n = p_1^{s_1} p_2^{s_2} ... p_t^{s_t}$. Then $\phi(n) = p_1^{s_1 - 1} p_2^{s_2 - 1} ... p_t^{s_t - 1} \phi(p_1 ... p_t)$. If $d|n$, then we may write $d = p_1^{r_1} p_2^{r_2} ... p_t^{r_t}$ and $\phi(d) = p_1^{r_1 - 1} p_2^{r_2 - 1} ... p_t^{r_t - 1} \phi(\prod_{i: r_i \neq 0} p_i)$, where $0 \leq r_i \leq s_i$ for all i. It is obvious that $\phi(d)|\phi(n)$, hence the claim.

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

1. The equivalence classes are $\overline{a} = \{a + 18k | k \in \mathbb{Z}\}$ where $a = 0, 1, ..., 17$.

2. For fixed integer n, all integers a may be written in the form $a = qn + r$, where $0 \leq r < |n|$ and $r, q \in \mathbb{Z}$. That is to say, $a - r = qn$ and therefore $n | a - r$. We can then say that a is in the residue class of r. The possible values of r are exactly $0, 1, ..., n-1$. So the distinct equivalence classes are exactly $\overline{0}, \overline{1}, ..., \overline{n-1}$.

These equivalence classes are truly distinct. If an integer a is in the equivalence class of both b and c, where $b \neq c$ and $0 \leq b, c < |n|$, then $a - b = q_b n$ and $a - c = q_c n$. It follows that $b - c = (q_c - q_b)n$. However, $|b - c| < |n|$ so this can only be true if $b - c = 0$, which is a contradiction.

3. Since $10 \equiv 1 \pmod 9$, we have that $10^n \equiv 1 \pmod 9$.Then $a_n 10^n \equiv a_n \pmod 9$, and $a \equiv a_n + a_{n-1} + ... + a_0 \pmod 9$.

4. First, note that $37 \equiv 8 \pmod{29}$ and that $8^{28} \equiv 1 \pmod{29}$. Then $37^{100} = 37^{3 \cdot 28 + 16} \equiv 8^{16} \equiv 23 \pmod{29}$. The remainder is 23.

5. The last two digits are the remainder when 9^{1500} is divided by 100. Note that $9^{10} \equiv 1 \pmod{100}$. Therefore, the last two digits are 01.

6. $\overline{0}^2 = \overline{0^2} = \overline{0}$, $\overline{1}^2 = \overline{1^2} = \overline{1}$, $\overline{2}^2 = \overline{2^2} = \overline{4} = \overline{0}$, and $\overline{3}^2 = \overline{3^2} = \overline{9} = \overline{1}$

7. From the previous exercise, we know that $\overline{a^2}, \overline{b^2}$ are either $\overline{0}$ or $\overline{1}$. Thus, $\overline{a^2 + b^2}$ must be $\overline{0}$, $\overline{1}$, or $\overline{2}$.

8. Consider the equation mod 4, and suppose that there exists non-zero integers a_0, b_0, and c_0 such that $a_0^2 + b_0^2 = 3c_0^2$. From the previous two exercises, we know that $\overline{3c_0^2}$ must be equal to either $\overline{0}$ or $\overline{3}$. However, since it is impossible for $\overline{a_0^2 + b_0^2}$ to be equal to $\overline{3}$, we find that both are equal to $\overline{0}$. Then we may write $a_0 = 2a_1$, $b_0 = 2b_1$, and $c_0 = 2c_1$, where $a_1, b_1, c_1 \in \mathbb{Z}$. It is clear that a_1, b_1, and c_1 are also solutions to the equation and that we can repeat this process infinitely many times to obtain an infinite number of solutions between 0 and a_0, b_0, c_0. This is absurd, hence there are no non-zero integer solutions to $a^2 + b^2 = 3c^2$.

9. Any odd integer may be written in the form $2k + 1$, where $k \in \mathbb{Z}$. The square of an odd integer is therefore $(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$. Note that if k is not even, then $k + 1$ must be so that for all $k \in \mathbb{Z}$, $(2k+1)^2 = 8q + 1$, for some integer q.

10. Proposition 4 states that $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} | (a,n) = 1\}$. From the first exercise, we know that the residue classes of $\mathbb{Z}/n\mathbb{Z}$ are $\overline{0}, \overline{1}, ..., \overline{n-1}$. Furthermore, we know that the number of integers a such that $a \leq n$ and $(a,n) = 1$ is $\phi(n)$. Therefore, there are $\phi(n)$ elements of $(\mathbb{Z}/n\mathbb{Z})^\times$.

11. If $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then there exist $\overline{a^{-1}}, \overline{b^{-1}} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{a^{-1}} \cdot \overline{a} = \overline{1}$ and $\overline{b^{-1}} \cdot \overline{b} = \overline{1}$. Observe that $\overline{b^{-1}} \cdot \overline{a^{-1}} \cdot \overline{a} \cdot \overline{b} = \overline{1}$ and that $\overline{a} \cdot \overline{b}, \overline{b^{-1}} \cdot \overline{a^{-1}} \in \mathbb{Z}/n\mathbb{Z}$. It follows that $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$

12. Let $a, n \in \mathbb{Z}$ such that $n > 1$ and $1 \leq a \leq n$. Suppose that $(a,n) = d$, $d > 1$. We may then write $n = bd$ and $a = cd$, where $b, c \in \mathbb{Z}$. Then $ab = cdb = cn \equiv 0 \pmod{n}$.

Now suppose that there exists $e \in \mathbb{Z}$ such that $ae \equiv 1 \pmod{n}$. Then $ae = qn + 1$ for some $q \in \mathbb{Z}$. Remembering that $n = bd$ and $a = cd$, we have $cde - qbd = d(ce - qb) = 1$. However $d > 1$ so $d \nmid 1$, which is a contradiction. Therefore, no such integer e exists.

13. Let $a, n \in \mathbb{Z}$ such that $n > 1$ and $1 \leq a \leq n$. Suppose that $(a,n) = 1$. Then there exist $b, c \in \mathbb{Z}$ such that $ac + nb = 1$ or $ac = -bn + 1$. Clearly, $ac \equiv 1 \pmod{n}$.

14. In the previous two exercises, we found that for $\overline{a}$, there exists $\overline{c}$ such that $\overline{a} \cdot \overline{c} = \overline{1}$ iff a and n are relatively prime. Therefore, $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{there exists } c \in \mathbb{Z}/n\mathbb{Z} \text{ with } \overline{a} \cdot \overline{c} = \overline{1}\} = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a,n) = 1\}$.

15. (a) 13 is prime and 20 is not a multiple of 13 so they are relatively prime. The multiplicative inverse of $\overline{13}$ is $\overline{17}$.

15. (b) 89 is prime so 69 and 89 are relatively prime. The multiplicative inverse of $\overline{69}$ is $\overline{40}$.

15. (c) 3797 is prime so 1891 and 3797 are relatively prime. The multiplicative inverse of $\overline{1891}$ is $\overline{253}$.

15. (d) 77695236973 is prime so 77695236973 and 6003722857 are relatively prime. The multiplicative inverse of $\overline{6003722857}$ is $\overline{77695236753}$.

16. This is trivial and is left as an exercise to the reader.