Dummit & Foote Abstract Algebra 3rd Ed

October 31, 2013

Chapter 0

0.1.1

This exercise is contained within 0.1.4

0.1.2

$(Q+P)X = QX + PX = XQ + XP = X(Q+P)$ Thus $(Q+P) \in B$

0.1.3

$(QP)X = Q(PX) = Q(XP) = (QX)P = (XQ)P = X(QP)$ Thus $(QP) \in B$

0.1.4

Take $p, q, r, s \in \Re$ s.t.

$A = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ and $AX = XA \implies \begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix} = \begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix}$

From here, we compare the entries on either side; we see $p = p + r \implies r = 0$,
and $p + q = q + s \implies p = s$

Thus the general form for $A \in B$ is $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$

As a sanity check, we check $AX = XA$ and get $\begin{pmatrix} a & a+b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a & a+b \\ 0 & a \end{pmatrix}$

0.1.5

(a) No, take $f(1/2) = 1$ and $f(2/4) = 2$, thus $a = a \not\Rightarrow f(a) = f(a)$
(b) Yes, since there is no information lost in this map, it must be well defined (i.e. you aren't throwing away any piece of the input)

0.1.6

This is a well defined map; each real number has a unique decimal representation, thus there is no way to change the first digit after the decimal point.

0.1.7

This relation is predicated on the = relation under the image of f, so this is clearly a equivalence relation, but we will show the properties nonetheless:

Reflexive - $a \sim a \implies f(a) = f(a)$ ✓

Symmetric - $a \sim b \implies f(a) = f(b) \implies f(b) = f(a) \implies b \sim a$ ✓

Transitive - $a \sim b,\ b \sim c \implies f(a) = f(b),\ f(b) = f(c) \implies f(a) = f(c) \implies a \sim c$ ✓

This relation is the definition of a fiber, as it relates all elements of the domain with the same value under f. If f were not surjective, we could find some element $b \in B$ such that $f(a) \neq b\ \forall a \in A$, and the fiber of f over b is the empty set. This empty set breaks our equivalence partitioning for our relation; however if we restrict f to surjection, the relation partitions A nicely into equivalence classes!

0.2.1

Syntax: $ax + by = gcd; lcm = (xy)/gcd$

(a) $2 * 20 + (-3) * 13 = 1; lcm = (20 * 13)$

(b) $27 * 69 + (-5) * 372 = 3; lcm = (23 * 372)$

(c) $8 * 792 + (-23) * 275 = 11; lcm = (792 * 25)$

(d) $(-126) * 11391 + 253 * 5673 = 3; lcm = (3797 * 5673)$

(e) $(-105) * 1761 + 118 * 1567 = 1; lcm = (1761 * 1567)$

(f) $(-17) * 507885 + 142 * 60808 = 691; lcm = (735 * 60808)$

0.2.2

We have for $a, b, n, m \in \mathbb{Z}; a = nk;\ b = mk \implies as + bt = (nk)s + (mk)t = k(ns + mt)$ and k divides $as + bt\ \forall s, t \in \mathbb{Z}$

0.2.3

We have $n = mk$ for some $m, k \in \mathbb{Z}$. Take $a = mq$ and $b = kp$ where $k \not| q$ and $m \not| p$, thus $n \not| a$ and $n \not| b$. Consider $ab = mqkp = (mk)qp = n(qp) \implies n|ab$

0.2.4

$ax+by = a(x_0+\frac{b}{d}t)+b(y_0-\frac{a}{d}t) = ax_0+\frac{ab}{d}t+by_0-\frac{ab}{d}t = ax_0+by_0+(\frac{ab}{d}-\frac{ab}{d})t = ax_0+by_0+0t;$ this is clearly invariant under choice of t and represents a valid solution space.

0.2.5

$\varphi(1) = 1;\ \varphi(2) = 1;\ \varphi(3) = 2;\ \varphi(4) = 2;\ \varphi(5) = 4;$

$\varphi(6) = 2;\ \varphi(7) = 6;\ \varphi(8) = 4;\ \varphi(9) = 6;\ \varphi(10) = 4;$

$\varphi(11) = 10;\ \varphi(12) = 4;\ \varphi(13) = 12;\ \varphi(14) = 6;\ \varphi(15) = 8;$

$\varphi(16) = 8;\ \varphi(17) = 16;\ \varphi(18) = 6;\ \varphi(19) = 18;\ \varphi(20) = 8;$

$\varphi(21) = 12;\ \varphi(22) = 10;\ \varphi(23) = 22;\ \varphi(24) = 8;\ \varphi(25) = 20;$

$\varphi(26) = 12;\ \varphi(27) = 18;\ \varphi(28) = 12;\ \varphi(29) = 28;\ \varphi(30) = 8;$

0.2.6

Take $S \subset \mathbb{N}$ and P to be the complement of S with $1 \in S$ and $s \in S \implies s+1 \in S$
Now take $p \in P$ such that p is the minimal element in P. We know $p \neq 1$ since $1 \in S$
Thus $p-1$ exists and can't be in P since p is the minimal element of P. $p-1 \notin P \implies p-1 \in S \implies p-1+1 = p \in S$. From here we see p is in S and the complement of S and can not exist, Thus P must be empty and $S = \mathbb{N}$

0.2.7

The power of p in pb^2 is bound to be odd, where the power of p in a^2 is bound to be even.
More explicitly,taking $a, b \in \mathbb{Z}$ we can write $a = k_1^{a_1} \dots k_n^{a_n} p^{a_p}; b = q_1^{b_1} \dots q_n^{b_n} p^{b_p}$ where q_i, k_i are primes. This means $a^2 = k_1^{2a_1} \dots k_n^{2a_n} p^{2a_p}$ and $pb^2 = q_1^{2b_1} \dots q_n^{2b_n} p^{2b_p+1}$, so we need to find a_p, b_p s.t. $2a_p = 2b_p + 1$ though this is impossible.

0.2.8

First we start by counting up to n by multiples of p. Note there are $\left\lfloor \frac{n}{p} \right\rfloor$ such numbers. At this point, we have counted up all single multiples of p, though we have yet to account for the multiples of p^2 (i.e. every p^{th} multiple of p). In order to get the number of p^2 terms, we count up to n over multiples of p^2 for a total number of $\left\lfloor \frac{n}{p^2} \right\rfloor$ (looks familiar). This counting method continues up to the ith power. Now to arrive at the largest power of p that divides into n, we sum up all these terms: $\sum\limits_{i \in \mathbb{N}} \left\lfloor \frac{n}{p^i} \right\rfloor$

0.2.9

Haskell implementation
$linearGCD :: Int -> Int -> (Int, Int, Int)$
$linearGCD\ a\ b = (d, u, v)\ where$
$\quad (d, x, y) = eGCD\ 0\ 1\ 1\ 0\ (abs\ a)\ (abs\ b)$
$\quad u \mid a < 0 = negate\ x$
$\quad\quad \mid otherwise = x$
$\quad v \mid b < 0 = negate\ y$
$\quad\quad \mid otherwise = y$
$\quad eGCD\ n1\ o1\ n2\ o2\ r\ s$
$\quad\quad \mid (s == 0) = (r, o1, o2)$
$\quad\quad \mid otherwise = case\ r\ `quotRem`\ s\ of$
$\quad\quad\quad (q, t) -> eGCD\ (o1 - q * n1)\ n1\ (o2 - q * n2)\ n2\ s\ t$

0.2.10

Let p be a prime larger than $N+1$ such that $\varphi(p^k) = (p-1)(p^{k-1}) > N$. Therefore any prime q dividing n is no larger than $N+1$ and there are only finitely many choices for this q. Furthermore, we know $\varphi(n) = \varphi(q^k)\varphi(m)$ for some number m that is not divisible by q. Note that $\varphi(m)$ is constant, so this equation relies on k. This limits $k \leq log_q(\frac{N}{m})$. Now we see that both the choice for q and k are of a finite set, thus there are finitely many numbers such that $\varphi(n) = N$.

Let's say there is some number M such that $\varphi(n) < M \forall n \in \mathbb{N}$. Since we are mapping an infinite set, $\mathbb{N}$, onto a finite set, we are bound to break the finite ceiling we set in the last previous portion (i.e. at least one of the numbers from $1 \dots M$ will have an infinite amount of numbers mapped to it). Thus we may not incur a maximum M.

0.2.11

Take $d = p_1^{a_1} \dots p_n^{a_n}$ where p_i is a prime that divides d. Since $d|n$, $n = p_1^{b_1} \dots p_n^{b_n} q$ where $a_i \leq b_i$.
From here, $\varphi(d) = \varphi(p_1^{a_1}) \dots \varphi(p_n^{a_n}) = p_1^{a_1 - 1} \dots p_n^{a_n - 1}(p_1 - 1) \dots (p_n - 1)$ and
$\varphi(n) = \varphi(p_1^{b_1})\varphi(p_2^{b_2}) \dots \varphi(p_n^{b_n})\varphi(q) = p_1^{b_1 - 1} \dots p_n^{b_n - 1}(p_1 - 1) \dots (p_n - 1)\varphi(q)$
Now since $a_i - 1 \leq b_i - 1$, $\varphi(d)|\varphi(n)$

0.3.1

$\mathbb{Z}/18\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}\}$
Where $\overline{a} = \{x \in \mathbb{Z} | x = 18k + a\}$

0.3.2

0.3.3

0.3.4

0.3.5

0.3.6

0.3.7

0.3.8

0.3.9

0.3.10

0.3.11

0.3.12

0.3.13

0.3.14

0.3.15

0.3.16

Chapter 1