

# Solutions to Homework Assignment 1

Daniel Mathews

October 7, 2004

## Section 1.1, Problem 1.

- (i) This is not associative as, in general

$$\begin{aligned}(a \star b) \star c &= (a - b) - c = a - b - c \\ a \star (b \star c) &= a - (b - c) = a - b + c\end{aligned}$$

which are clearly not always equal.

- (ii) This can be computed explicitly but it is quicker if we note that any real number can be written in the form  $x - 1$ . Then we obtain  $(a - 1) \star (b - 1) = ab - 1$  for any  $a, b \in \mathbb{R}$ . We have

$$\begin{aligned}[(a - 1) \star (b - 1)] \star (c - 1) &= (ab - 1) \star (c - 1) = abc - 1 \\ (a - 1) \star [(b - 1) \star (c - 1)] &= (a - 1) \star (bc - 1) = abc - 1\end{aligned}$$

so that the operation is associative.

- (iii) This is not associative. We compute

$$\begin{aligned}(a \star b) \star c &= \frac{a + b}{5} \star c = \frac{\frac{a+b}{5} + c}{5} = \frac{a}{25} + \frac{b}{25} + \frac{c}{5} \\ a \star (b \star c) &= a \star \frac{b + c}{5} = \frac{a + \frac{b+c}{5}}{5} = \frac{a}{5} + \frac{b}{25} + \frac{c}{25}\end{aligned}$$

## Section 1.1, Problem 2.

- (i) The operation is clearly not commutative, as in general, for  $a \neq b \in \mathbb{Z}$ ,  $a - b \neq b - a$ .
- (ii) The operation is commutative as  $a \star b = a + b + ab = b + a + ba = b \star a$ .
- (iii) The operation is commutative as  $a \star b = \frac{a+b}{5} = \frac{b+a}{5} = b \star a$ .

**Section 1.1, Problem 25.**

Take  $x, y \in G$ . We wish to show  $xy = yx$ . From the given condition we have  $x^2 = 1$ ,  $y^2 = 1$ , and  $(xy)^2 = xyxy = 1$ . From  $xyxy = 1$  we multiply on the left by  $x$ , and since  $x^2 = 1$ , we obtain  $yxxy = x$ . Now multiply on the left by  $y$  and use  $y^2 = 1$  to obtain  $xy = yx$ , as required.

**Section 1.2, Problem 3.**

The elements of  $D_{2n}$  can be written out:

$$D_{2n} = \{1, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\},$$

so an element of  $D_{2n}$  which is not a power of  $r$  is of the form  $sr^i$  where  $0 \leq i \leq n-1$ . Now clearly any such element is not the identity, so it suffices to show that, for  $0 \leq i \leq n-1$ , we have  $(sr^i)^2 = sr^i sr^i = 1$ . But since  $r^i s = sr^{-i}$ , we have  $sr^i sr^i = s(r^i s)r^i = s(sr^{-i})r^i = s^2 = 1$ , as required. Now  $sr$  and  $s$  generate  $D_{2n}$ : we easily obtain  $s$  and  $r = s^{-1}sr$ , and it is clear (for example, from the standard presentation of  $D_{2n}$  that  $r, s$  generate  $D_{2n}$ ).

**Section 1.2, Problem 4.**

We have  $n = 2k$  so that  $z = r^k \in D_{2n}$  has order 2: it is not the identity, and  $z^2 = r^{2k} = r^n = 1$ . We refer to the list of elements of  $D_{2n}$  above and show that  $z$  commutes with each of these elements. First consider  $r^i$ , where  $0 \leq i \leq n-1$  (this includes the identity element): then  $r^i z = r^i r^k = r^{i+k} = r^k r^i = z r^i$ . Then consider  $sr^i$ , where  $0 \leq i \leq n-1$ : we have

$$sr^i z = sr^i r^k = sr^{i+k} = (sr^k)r^i = (r^{-k}s)r^i = r^{2k}r^{-k}sr^i = r^k sr^i = z sr^i.$$

The equalities follow from standard algebraic manipulation, and the fact that  $sr^k = r^{-k}s$ , and the fact that  $r^{2k} = r^n = 1$ . So  $z$  commutes with every element of  $D_{2n}$ .

We now must show that for every element  $y$  of  $D_{2n}$  other than 1 or  $z$ ,  $y$  does not commute with all elements of  $D_{2n}$ . That is, for every  $y \in D_{2n}$  not equal to 1 or  $z$ , we find an element of  $D_{2n}$  that does not commute with  $y$ . Again we refer to the list of elements of  $D_{2n}$  to consider the possibilities for  $y$ : either  $y = r^i$  for some  $i$ , or  $y = sr^i$  for some  $i$ .

First suppose that  $y = r^i$  where  $1 \leq i \leq n-1$  and  $i \neq k$ . We show that  $y$  does not commute with  $s$ . We prove this by contradiction, so assume that  $ys = sy$ , i.e.,  $r^i s = sr^i$ . But we know that  $r^i s = sr^{-i}$ , so we obtain  $sr^{-i} = sr^i$ , and cancelling  $s$ 's (i.e. multiplying on the left by  $s^{-1}$ ) we obtain  $r^{-i} = r^i$ , and hence  $r^{2i} = 1$ . But recall that  $1 \leq i \leq n-1$ , so that  $2 \leq 2i \leq 2n-2$ . Since  $r^1, \dots, r^{n-1} \neq 1$ , and  $r^n = 1$ , and  $r^{n+i} = r^i$ , we must have  $2i = n$ , so that  $i = k$ , a contradiction since we assumed  $i \neq k$ . It follows that  $y = r^i$  does not commute with  $s$ .

Second suppose that  $y = sr^i$  where  $0 \leq i \leq n-1$ . We show that  $y$  does not commute with  $r$ . We prove this by contradiction again, so assume  $yr = ry$ , i.e.  $sr^i r = r sr^i$ . Since  $rs = sr^{-1}$  we obtain  $sr^{i+1} = sr^{i-1}$ , and cancelling  $s$ 's gives  $r^{i+1} = r^{i-1}$ . Cancelling  $i-1$   $r$ 's from both sides then gives  $r^2 = 1$ . But this cannot be true unless  $n$  is 1 or 2. But we are given that  $n \geq 4$ , a contradiction. Therefore  $y = sr^i$  does not commute with  $r$ .

Now we have shown that for every  $y \neq 1, z$  in  $D_{2n}$ ,  $y$  does not commute with every element of  $D_{2n}$ , as required.

**Section 1.3, Problem 11.**

The permutation  $\sigma$  can be visualised by placing the numbers  $1, 2, \dots, m$  clockwise around a circle, then  $\sigma$  takes each number to the one next to it clockwise. Equivalently,  $\sigma$  takes the number  $k$  to  $k + 1$ , considered modulo  $m$ . We see then that  $\sigma^i$  takes each number to the one  $i$  places around clockwise from it, so takes the number  $k$  to  $k + i$  modulo  $m$ . So  $\sigma^i$  takes the number 1 to  $i + 1$  modulo  $m$ ; takes  $i + 1$  to  $2i + 1$  modulo  $m$ ; and so on. Thus one of the cycles of  $\sigma^i$  is  $(1 \ i + 1 \ 2i + 1 \ \dots)$ . If this cycle has length  $m$ , then it must be the only cycle (since all the numbers from 1 to  $m$  must be in it), so that  $\sigma^i$  is an  $m$ -cycle. If this cycle has length less than  $m$ , then there must be more than one cycle and  $\sigma^i$  is not an  $m$ -cycle.

So we ask: how long is the cycle of  $\sigma^i$  starting with 1? Calling this cycle length  $k$ , we see that  $k$  is the smallest positive integer such that  $1 + ik \cong 1 \pmod m$ . Equivalently,  $k$  is the smallest positive integer such that  $m | ik$ . If  $i$  is relatively prime to  $m$ , then  $m | ik$  implies  $m | k$ , so that the smallest such  $k$  is  $k = m$ . If  $i$  is not relatively prime to  $m$  then let  $d$  be the highest common factor of  $i$  and  $M$ . So  $m = dm'$  and  $i = di'$  for some relatively prime positive integers  $m', i'$ . Then the question becomes: what is the smallest positive integer  $k$  such that  $dm' | di'k$ , or equivalently,  $m' | i'k$ ? Since  $m', i'$  are relatively prime, the smallest such  $k$  is  $k = m'$ .

We have shown that if  $i$  is relatively prime to  $m$  then  $\sigma^i$  is an  $m$ -cycle. On the other hand, if  $i$  is not relatively prime to  $m$ , then  $\sigma^i$  contains an  $m'$ -cycle, for some  $m' < m$ , so cannot be an  $m$ -cycle.

**Section 1.4, Problem 1.**

Denote the two elements of  $\mathbb{F}_2$  by 0, 1, which operate according to the laws of multiplication, addition, and division modulo 2. The group  $GL_2(\mathbb{F}_2)$  consists of those matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

such that  $a, b, c, d \in \mathbb{F}_2$  and  $ad - bc \neq 0$ , which is equivalent to  $ad - bc = 1$ . Thus the order of  $GL_2(\mathbb{F}_2)$  is equal to the number of solutions  $(a, b, c, d)$  to the equation  $ad - bc = 1$ .

We now enumerate those solutions. Either  $ad = 1, bc = 0$  or  $ad = 0, bc = 1$ . In the first case we have  $a = d = 1$  and three possibilities  $(b, c) = (0, 0), (0, 1), (1, 0)$ . In the second case we have  $bc = 1$  and  $(a, d) = (0, 0), (0, 1), (1, 0)$ . This gives six solutions, so  $|GL_2(\mathbb{F}_2)| = 6$ .

**Section 1.4, Problem 11.**

For ease of notation, we will denote by  $M(a, b, c)$  the matrix

$$M(a, b, c) = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}.$$

Thus  $H(F)$  consists precisely of the matrices  $M(a, b, c)$  with  $a, b, c \in F$ .

- (i) Explicitly we compute  $M(a, b, c)M(d, e, f) = M(a + d, b + e + af, c + f)$ :

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a + d & b + e + af \\ 0 & 1 & c + f \\ 0 & 0 & 1 \end{bmatrix}.$$

So  $H(F)$  is closed under matrix multiplication. To see that  $H(F)$  is non-abelian, we take the 0 and 1 elements of  $F$  and form  $X = M(0, 0, 1)$ ,  $Y = M(1, 0, 0)$ . Then the rule computed above tells us  $XY = M(1, 0, 1)$  but  $YX = (1, 1, 1)$  so  $XY \neq YX$ .

- (ii) The identity in  $H(F)$  is clearly the identity matrix  $M(0, 0, 0)$ . Given  $X = M(a, b, c)$ , we need to find an inverse  $X^{-1} = M(d, e, f)$  such that  $M(a, b, c)M(d, e, f) = M(0, 0, 0)$ . From the multiplication rule computed above we obtain  $a + d = 0$ ,  $b + e + af = 0$ ,  $c + f = 0$ . From the first and last of these we obtain  $d = -a$  and  $f = -c$ . Then the second equation gives  $e = -b - af = ac - b$ . Checking, we see that  $M(a, b, c)M(-a, ac - b, -c) = M(-a, ac - b, -c)M(a, b, c) = M(0, 0, 0)$ , which is the identity, so we have found an inverse  $X^{-1} = M(-a, ac - b, -c)$ .
- (iii) We now prove the associative law for  $H(F)$ . So take three elements  $X = M(a, b, c)$ ,  $Y = M(d, e, f)$ ,  $Z = M(g, h, i)$  in  $H(F)$ . We have

$$\begin{aligned} (XY)Z &= (M(a, b, c)M(d, e, f))M(g, h, i) \\ &= M(a + d, b + e + af, c + f)M(g, h, i) \\ &= M(a + d + g, b + e + af + h + ai + di, c + f + i) \\ X(YZ) &= M(a, b, c)(M(d, e, f)M(g, h, i)) \\ &= M(a, b, c)M(d + g, e + h + di, f + i) \\ &= M(a + d + g, b + e + h + di + af + ai, c + f + i) \end{aligned}$$

which are equal, since  $a$  thru  $i$  are elements of the field  $F$ .

Now we have proved that  $H(F)$  is closed under matrix multiplication, which is associative. There is an identity, and every element has an inverse. Thus  $H(F)$  forms a group under matrix multiplication. Since every element is of the form  $M(a, b, c)$  with  $a, b, c \in F$ , and since every  $a, b, c \in F$  give an element  $M(a, b, c)$ , the number of elements in  $H(F)$  is equal to  $|F|^3$ :  $|F|$  choices for  $a$ ,  $|F|$  choices for  $b$ , and  $|F|$  choices for  $c$ .

- (iv) The group  $H(\mathbb{Z}/2\mathbb{Z})$  has 8 elements by the previous part. We see that  $M(a, b, c)^2 = M(a + a, b + b + ac, c + c) = M(0, ac, 0)$  since in  $\mathbb{Z}/2\mathbb{Z}$ ,  $0 + 0 = 1 + 1 = 0$ . Obviously the only element with order 1 is the identity  $M(0, 0, 0)$ . We see that if  $ac = 0$  then  $M(a, b, c)^2$  is the identity, so if  $ac = 0$  but  $a, b, c$  are not all 0 then  $M(a, b, c)$  has order 2. Thus  $M(0, 0, 1)$ ,  $M(0, 1, 0)$ ,  $M(0, 1, 1)$ ,  $M(1, 0, 0)$ ,  $M(1, 1, 0)$  are all of order 2. This leaves

only two elements:  $M(1, 0, 1)$  and  $M(1, 1, 1)$ . We compute

$$\begin{aligned} M(1, 0, 1)^2 &= M(0, 1, 0), \\ M(1, 0, 1)^3 &= M(0, 1, 0)M(1, 0, 1) = M(1, 1, 1), \\ M(1, 0, 1)^4 &= M(0, 1, 0)^2 = M(0, 0, 0), \end{aligned}$$

so that  $M(1, 0, 1)$  has order 4. Similarly we see that  $M(1, 1, 1)$  has order  $r$ :

$$\begin{aligned} M(1, 1, 1)^2 &= M(0, 1, 0), \\ M(1, 1, 1)^3 &= M(0, 1, 0)M(1, 1, 1) = M(1, 0, 1), \\ M(1, 1, 1)^4 &= M(0, 1, 0)^2 = M(0, 0, 0). \end{aligned}$$

- (v) We prove that the only element of  $H(\mathbb{R})$  with finite order is the identity. So take  $M(a, b, c) \in H(\mathbb{R})$  which has finite order. Then for some positive integer  $n$ ,  $M(a, b, c)^n = M(0, 0, 0)$ . Checking a few examples suggests the following claim:  $M(a, b, c)^n$  is of the form  $M(na, *, nc)$ . This is clearly true for  $n = 1$ . Suppose it is true for  $n = k$ , so that  $M(a, b, c)^k = M(ka, x, kc)$  for some  $x \in \mathbb{R}$ . Then  $M(a, b, c)^{k+1} = M(ka, x, kc)M(a, b, c) = M((k+1)a, x + b + kac, (k+1)c)$ , which has the desired form, proving the claim by induction. Thus if  $M(a, b, c)^n = M(0, 0, 0)$ , then  $na = nc = 0$ . As  $n$  is a positive integer we have  $a = c = 0$ , and  $M(a, b, c) = M(0, b, 0)$ . Again an example suggests a claim:  $M(0, b, 0)^n = M(0, nb, 0)$ . This is true for  $n = 1$ . Suppose it is true for  $n = k$ . Then  $M(0, b, 0)^{k+1} = M(0, kb, 0)M(0, b, 0) = M(0, (k+1)b, 0)$ , proving the claim by induction. Now if  $M(0, b, 0)^n$  is the identity, then  $nb = 0$ , and as  $n$  is a positive integer,  $b = 0$ . Thus  $M(a, b, c) = M(0, 0, 0)$  is the identity. So the only element of  $H(\mathbb{R})$  with finite order is the identity.

### Section 1.5, Problem 1.

Obviously 1 has order 1, and  $-1$  has order 2 since  $(-1)^2 = 1$ . Now  $i^2 = -1$ ,  $i^3 = -i$ ,  $i^4 = 1$  so  $i$  has order 4. Similarly, if  $x$  is any of  $j, k, -i, -j, -k$ , then  $x^2 = -1$ , so that  $x^3 = x^2 \cdot x = -x$  and  $x^4 = (x^2)^2 = (-1)^2 = 1$ . Thus  $j, k, -i, -j, -k$  all have order 4.

#### Class problem 1.

We have a set  $G$  with an associative operation  $G \times G \rightarrow G$ . There is a one-sided identity  $e$  such that for all  $a \in G$  we have  $ae = a$ . And each  $a \in G$  has a one-sided inverse  $a^{-1}$  such that  $aa^{-1} = e$ . To show  $G$  is a group we show that  $a^{-1}$  is actually a two-sided inverse, and  $e$  is actually a two-sided identity.

Given  $a \in G$ , we have

$$a^{-1}a = a^{-1}aa^{-1}(a^{-1})^{-1} = a^{-1}(a^{-1})^{-1} = e$$

so that  $aa^{-1} = a^{-1}a$  and  $a$  is a two-sided identity. We also have, for any  $a \in G$ ,

$$ea = aa^{-1}a = a(a^{-1}a) = ae = a,$$

so that  $ae = ea = a$  and  $e$  is a two-sided identity. Thus  $G$  forms a group.

**Class problem 2.**

We consider the two possible perfectly interleaving shuffles of a deck of cards. Numbering the cards from 1 to 52, the two permutations are given by

$$1 \mapsto 1, \quad 2 \mapsto 3, \quad 3 \mapsto 5, \dots, 26 \mapsto 51, \quad 27 \mapsto 2, \quad 28 \mapsto 4, \dots, 52 \mapsto 52$$

and

$$1 \mapsto 2, \quad 2 \mapsto 4, \quad 3 \mapsto 6, \dots, 26 \mapsto 52, \quad 27 \mapsto 1, \quad 28 \mapsto 3, \dots, 52 \mapsto 51.$$

One way to find the order of these permutations is to write out their cycle structure explicitly and compute the order as the least common multiple of the cycle lengths. However we take a different route.

The first permutation can be described by the map  $\varphi : x \mapsto 2x - 1$ , where numbers are considered modulo 51. The order of the permutation is equal to the least positive integer  $i$  such that  $\varphi^i(x) = x$ . We can compute

$$\begin{aligned} \varphi^2(x) &= 4x - 3, & \varphi^3(x) &= 8x - 7, & \varphi^4(x) &= 16x - 15, & \varphi^5(x) &= 32x - 31, \\ \varphi^6(x) &= 13x - 12, & \varphi^7(x) &= 26x - 25, & \varphi^8(x) &= x, \end{aligned}$$

so the order of the permutation is 8.

Now consider the second permutation, which can be described by the map  $\psi : x \mapsto 2x$  modulo 53. Since  $\psi^i(0) = 0$ , the order of the permutation is equal to the least  $i$  such that  $\psi^i(x) = x$ . But clearly  $\psi^i(x) = 2^i x \pmod{53}$ . Since 53 is a prime, and  $x \neq 0$  we have  $2^i x \equiv x \pmod{53}$  if and only if  $2^i \equiv 1 \pmod{53}$ . By Fermat's little theorem we have  $2^{52} \equiv 1 \pmod{53}$ , so the answer is a factor of 52. However we can compute

$$2^2 \equiv 4 \pmod{53}, \quad 2^4 \equiv 16 \pmod{53}, \quad 2^{13} \equiv 30 \pmod{53}, \quad 2^{26} \equiv -1 \pmod{53}$$

so that the answer must be 52. Thus the permutation has order 52.