

## MODEL ANSWERS TO THE FIRST HOMEWORK

1. Chapter 4, §1: 2. Suppose that  $F$  is a field and that  $a$  and  $b$  are in  $F$ . Suppose that

$$a \cdot b = 0,$$

and that  $b \neq 0$ . Let  $c$  be the inverse of  $b$ . Multiplying the equation above by  $c$  on the left, we get

$$\begin{aligned} 0 &= 0 \cdot c \\ &= (a \cdot b) \cdot c \\ &= a \cdot (b \cdot c) \\ &= a \cdot 1 \\ &= a. \end{aligned}$$

Thus  $a = 0$ . It follows that  $F$  is an integral domain.

8. We compute

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix},$$

and

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}.$$

If we have equality, then  $b = 0$  and  $c = 0$  and vice-versa. Thus the only matrices that commute with

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

are matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},$$

where  $a$  and  $b$  are arbitrary.

10. (a) One way to do this is to write down three general matrices and compute the triple product explicitly, both ways, and check that you get the same answer. A simpler, and possibly more aesthetically pleasing approach, is as follows. Note that a  $2 \times 2$  matrix  $A$  determines a map

$$f: \mathbb{R}^2 \longrightarrow \mathbb{R}^2,$$

where  $R^2 = R \times R$  is the ordinary cartesian product. Given  $v = (a, b) \in R^2$ , formally treat this as a column vector and define

$$f(a, b) = Av,$$

where  $Av$  is computed in the usual way. Note that, in these terms, the product of two matrices corresponds to composition of functions, and that  $f$  determines  $A$ ; indeed the first column of the matrix can be recovered from  $Av$ , where  $v = (1, 0)$  and the second column from  $Av$ , where  $v = (0, 1)$ . The fact that matrix multiplication is associative translates to the fact that composition of functions is associative.

(b) Clearly  $T$  is non-empty (for example it contains the zero matrix). Suppose that  $A$  and  $B$  are in  $T$ . Then

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}.$$

Then

$$A + B = \begin{pmatrix} a + a' & b + b' \\ 0 & c + c' \end{pmatrix} \quad \text{and} \quad AB = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix}$$

are both in  $T$ . Thus  $T$  is closed under addition and multiplication. As  $T$  also contains the identity matrix and its additive inverse,  $T$  is a subring.

(c) We employ the notation above. If  $AB$  is the identity, then  $aa' = cc' = 1$ . Thus  $a$  and  $c$  have inverses. Now suppose that  $a$  and  $c$  have inverses. Let

$$B = \begin{pmatrix} a^{-1} & a^{-1}bc^{-1} \\ 0 & c^{-1} \end{pmatrix}.$$

Then by the formulae above,  $B$  is the inverse of  $A$ .

14. A general quaternion is of the form  $q = a + bi + cj + dk$ . We have

$$qi = -b + ai + dj - ck \quad \text{and} \quad iq = -b + ai - dj + ck.$$

For these to be equal, we must have

$$d = -d \quad \text{and} \quad c = -c.$$

As  $c$  and  $d$  are real numbers, it follows that  $c = d = 0$ .

Thus the only quaternions that commute with  $i$  are of the form  $a + bi$ .

15. We have already seen that the only quaternions that commute with  $i$  are of the form  $a + bi$ . By symmetry, it follows that the only quaternions that commute with  $j$  are of the form  $a + cj$ .

Now the only quaternions, which are both of the form  $a + bi$  and  $a + cj$ , are in fact of the form  $a$ , that is, real numbers.

19. Suppose that  $x = a + bi + cj + dk$  and that  $x^2 = -1$ . Now the only numbers that multiply  $x$  to get a real number are multiples of the

complex conjugate of  $\bar{x} = a - bi - cj - dk$ . Thus  $a = 0$  and  $\bar{x} = -x$ . Thus

$$1 = -x^2 = x\bar{x} = b^2 + c^2 + d^2.$$

Clearly this has infinitely many solutions.

20. (a) As  $G$  is a finite subset of the multiplicative group of the quaternions, it suffices to prove that  $G$  is closed under products. To prove this, as  $(-a)b = a(-b) = -(ab)$ , it suffices to observe the product of any two of  $i, j$  and  $k$  is the third, up to sign.

(b) As the order of  $G$  is 8, by Lagrange, the order of a subgroup  $H$  is one, two, four, or eight.

If the order is one, then  $H = \{1\}$  and if the order is eight then  $H = G$ . Now the order of the elements  $\pm i, \pm j$  or  $\pm k$  of  $G$  is four. Thus  $G$  has three subgroups of order 4,  $\langle i \rangle, \langle j \rangle$  and  $\langle k \rangle$ . If  $H$  does not contain any of these elements, then the only other possibility is that  $H = \langle -1 \rangle$ .

(c) Note that  $i$  does not commute with  $j$ . By symmetry  $\pm i, \pm j$  and  $\pm k$  are not in the centre of  $G$ . On the other hand  $-1$  commutes with everything, so that the centre is equal to  $\langle -1 \rangle$ .

(d) Let  $H$  be a subgroup of  $G$ . If  $H = \{1\}$  or  $H = G$ , then  $H$  is automatically normal. If  $H$  has order two, then  $H$  is the centre, so that  $H$  is automatically normal. The only other case is if  $H$  has order 4. In this case  $H$  has index two and so  $H$  is automatically normal.

23 (a) We have

$$\begin{aligned} x^{**} &= (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)^{**} \\ &= (\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k)^* \\ &= \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \\ &= x. \end{aligned}$$

(b) We have

$$\begin{aligned} (x + y)^* &= (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k + \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k)^* \\ &= (\alpha_0 + \beta_0 + (\alpha_1 + \beta_1)i + (\alpha_2 + \beta_2)j + (\alpha_3 + \beta_3)k)^* \\ &= \alpha_0 + \beta_0 - (\alpha_1 + \beta_1)i - (\alpha_2 + \beta_2)j - (\alpha_3 + \beta_3)k \\ &= \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k + \beta_0 - \beta_1 i - \beta_2 j - \beta_3 k \\ &= x^* + y^*. \end{aligned}$$

(c) We have

$$\begin{aligned} xx^* &= (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)^* \\ &= (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) \\ &= \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2. \end{aligned}$$

This is visibly a non-negative real number. It is not hard to see that we get the same answer if we compute  $x^*x$ .

(d) We want to show

$$(xy)^* = y^*x^*.$$

We could show this directly, but this is a little bit tedious.

Here is a more conceptual way. If we fix  $x$  and consider the LHS and the RHS as functions of  $y$  then we get two functions  $L(y)$  and  $R(y)$  that depend on  $y$ . Note that  $L(y)$  is linear in  $y$ . This means

$$L(y_1 + y_2) = L(y_1) + L(y_2) \quad \text{and} \quad L(cy) = cL(y),$$

is  $c$  is a real number. The fact that  $L$  is linear follows from the fact that the two functions

$$y \longrightarrow xy \quad \text{and} \quad y \longrightarrow y^*$$

are linear and the fact that the composition of linear functions is linear. Similarly  $R(y)$  is linear, as the two functions

$$y \longrightarrow y^* \quad \text{and} \quad y \longrightarrow yx^*$$

are linear.

Note that the set

$$\{1, i, j, k\}$$

is a basis for the quaternions, as a real vector space. Thus it suffices to check that

$$(xy)^* = y^*x^* \quad \text{for} \quad y \in \{1, i, j, k\}.$$

Now consider fixing  $y$  and considering both sides of the equation as functions of  $x$ . As before both sides are linear and so it suffices to check that

$$(xy)^* = y^*x^* \quad \text{for} \quad x, y \in \{1, i, j, k\}.$$

Equality is clear if either  $x$  or  $y$  is 1. So we may suppose that

$$x, y \in \{i, j, k\}.$$

In this case the RHS is

$$\begin{aligned} y^*x^* &= (-y)(-x) \\ &= yx. \end{aligned}$$

So we have to check that

$$(xy)^* = yx \quad \text{for} \quad x, y \in \{i, j, k\}.$$

Equality is clear if  $x = y$ . Thus we may assume that

$$x, y \in \{i, j, k\} \quad \text{and} \quad x \neq y.$$

In this case  $xy = z$  is the third element of the set

$$\{i, j, k\},$$

up to sign.  $yx = -z$  is also the third element, with the opposite sign. Taking conjugates we get equality:

$$\begin{aligned}(xy)^* &= z^* \\ &= -z \\ &= yx.\end{aligned}$$

2. Chapter 4, §2: 2. If  $ab = ac$  then  $0 = ab - ac = a(b - c)$ . As  $R$  is an integral domain, and  $a \neq 0$ , it follows that  $b - c = 0$ , so that  $b = c$ .

3. See model answers to question 40.

8. (a) Denote by  $na$ ,  $a$  added to itself  $n$  times. Then if  $[n]$  denotes 1 added to itself  $n$  times, it is easy to see, but somewhat tedious to prove, that  $na = [n]a$ . Now as  $F$  is finite, there is an integer  $n$  (for example the order of  $F$ ) such that  $na = 0$ . It follows, as  $F$  is an integral domain, that  $[n] = 0$ . Suppose that  $n = xy$ . Then  $[n] = [x][y] = 0$  and as  $F$  is an integral domain, either  $[x] = 0$  or  $[y] = 0$ . In this case, it follows that if  $p$  is the smallest positive integer such that  $[p] = 0$  then  $p$  is prime. But then  $pa = [p]a = 0$ , for every  $a \in R$ .

(b) Suppose that the order of  $F$  is  $q$  and that  $q$  is not coprime to  $p$ . Pick a prime  $r$  that divides  $q$ . Then by Sylow's Theorems there is a subgroup of order  $r$ . If  $a$  is a generator of this subgroup then  $pa \neq 0$ , a contradiction.

33. (a) As  $G$  is a finite subset, it suffices to prove that  $G$  is a domain. Now the zero matrix has zero determinant. Thus it suffices to prove that the determinant of a product of two matrices is the product of the determinants. This can be easily checked.

(b) There are a number of ways to do this. The first, and perhaps the most elegant, is to use a little linear algebra; a  $n \times n$  matrix  $A$  has non-zero determinant if and only if its rows are linearly independent, that is, form a basis of the underlying vector space.

Thus we just need to count the number of bases. A basis consists of two linearly independent vectors. Think about picking these two vectors, one at a time. There are  $p^2$  vectors in total, as there are  $p$  choices for each coordinate. Of course, the only restriction for choosing the first vector  $v$ , is that we must not choose the origin.

Thus there are  $p^2 - 1$  choices for the first vector. Now consider picking the second vector  $w$ . The only requirement is that we don't pick a multiple of  $v$ , that is, a vector lying in the line spanned by  $v$ . But any line has  $p$  points, thus there are  $p^2 - p$  choices for  $w$ .

In total then there are  $(p^2 - 1)(p^2 - p)$  choices for  $A$ .

Another way to proceed is as follows. There are  $p^4$   $2 \times 2$  matrices, corresponding to the  $p$  choices for each of the four entries of  $A$ . But some of these will give us matrices with zero determinant. So it remains to count these. If the entries are  $a, b, c$  and  $d$ , we must count the number of solutions  $(a, b, c, d) \in \mathbb{F}_p$ ,

$$ad = bc.$$

There are two cases. Suppose that  $ad \neq 0$ . Then for every choice of  $b \neq 0$  there is a unique choice of  $c$  such that  $ad = bc$ .  $ad \neq 0$  is equivalent to  $a \neq 0, d \neq 0$ . Thus there are  $(p-1)^3$  solutions of this form. Otherwise  $ad = 0$ . In this case  $bc = 0$  as well. Thus we need to count the number of solutions of

$$ad = 0 \quad \text{and} \quad bc = 0.$$

Now the equation  $ad = 0$  has  $2p - 1$  solutions, for pairs  $(a, d)$ . Thus there are  $(2p - 1)^2$  solutions of  $ad = 0$  and  $bc = 0$ . In total then there are  $(p-1)^3 + (2p-1)^2$  solutions. So there are  $p^4 - (p-1)^3 - (2p-1)^2$   $2 \times 2$  matrices, with entries in  $\mathbb{F}_p$ .

(c) Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Suppose that  $A$  commutes with every element in  $G$ . Then in fact  $A$  must commute with every element in  $M_2(\mathbb{F}_p)$ . Indeed the point is that the invertible matrices generate the whole ring. Let

$$B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix},$$

and

$$BA = \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}.$$

Thus  $b = c = 0$ . On the other hand it is easy to see that any diagonal matrix commutes with every other matrix. Thus the centre of  $G$  is given by all matrices of the form

$$A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$

(d) The order of  $G$  is  $p(p-1)^2(p+1)$ . Thus a Sylow- $p$  subgroup has order  $p$ . The centre has order  $(p-1)^2$  so no subgroup of the centre will

work. In fact consider all matrices of the form

$$A(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

The product of  $A(a)$  and  $A(b)$  is easily seen to be  $A(a+b)$ . Thus these matrices are closed under products and so we do have a subgroup. On the other hand, as there are  $p$  choices for  $a$ , this is a subgroup of order  $p$ .

36. It suffices to exhibit a zero divisor. To eliminate ambiguity denote the  $i$  of  $\mathbb{C}$  by  $I$ . If  $p = a + bi + cj + dk$  is any quaternion, then

$$p\bar{p} = a^2 + b^2 + c^2 + d^2.$$

We want this to be equal to zero. Take  $a = 1$  and  $b = I$ . Thus  $p = 1 + Ii$  is a zero divisor as

$$(1 + Ii)(1 - Ii) = 0.$$

40. Let  $R$  be a finite domain. It suffices to prove that every non-zero element  $a$  has an inverse. Define a map

$$f: R \longrightarrow R$$

by the rule  $f(b) = ab$ . I claim that  $f$  is injective. Suppose not. Then  $f(b) = f(c)$ . But then  $ab = ac$ . In this case  $ab - ac = 0$  so that  $a(b - c) = 0$ . As  $a$  is non-zero and  $R$  is a domain,  $b - c = 0$ , so that  $b = c$ .

Thus  $f$  is injective. As  $f$  is injective and  $R$  is finite,  $f$  is surjective. Thus there is an element  $b \in R$  so that  $f(b) = 1$ , that is,  $ab = 1$ . Thus every element non-zero element of  $R$  has a right inverse. It follows that the non-zero elements of  $R$  form a group.

4. The trick here is to employ a heuristic and imagine that  $r$  is a real number. In this case we are looking for the inverse of  $(1 - r)$ ,

$$\frac{1}{1 - r}.$$

Note that this is the sum of a geometric series

$$\frac{1}{1 - r} = 1 + r + r^2 + r^2 + \cdots + r^n + \cdots,$$

with common ratio  $r$ , provided that  $|r| < 1$ .

In our case it does not make sense to think of convergence but we might hope the same piece of algebra works (or, if you like, in the context of real numbers,  $r^n = 0$  defines an infinitesimal, which is smaller than any positive real; thus we should have convergence).

Now  $r^n = 0$ , so we just look at the finite sum

$$a = 1 + r + r^2 + \cdots + r^{n-1}$$

and we compute

$$\begin{aligned}(1 - r) \cdot a &= a - ra \\ &= (1 + r + r^2 + \cdots + r^{n-1}) - (r + r^2 + r^3 + \cdots + r^n) \\ &= 1 - r^n \\ &= 1.\end{aligned}$$

Thus  $1 - r$  is invertible.