MODEL ANSWERS TO HWK #7

1. 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.

2. 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.

3. (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 2×2 matrix A determines a map

$$f \colon R^2 \longrightarrow R^2,$$

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 top row of the matrix can be recovered from Av, where $v = (1, 0)$ and the bottom row 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

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

Then

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

both in T. Thus T is closed under addition and multiplication. As T also contains the identity matrix and it is closed under inverses, 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.
4. A general quaternion is of the form $q = a + bi + cj + dk$. We have

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

For these to be equal, we must have

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

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 $a + bi$.
5. 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.
6. 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 conjugate $\bar{x} = a - bi - cj - dk$ of x. Hence $a = 0$ and $\bar{x} = -x$. Thus

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

Clearly this has infinitely many solutions.

7. Let R be all quaternions of the form $a + bi + cj + dk$, where a, b, c and d are integers. We first check that R is a ring; since it is a subset of the quaternions we just need to show that it is closed under addition and multiplication, which is clear.
It is clearly a domain, as it is a subring of a domain. i, $j \in R$ and

$$i \cdot j = k \neq -k = j \cdot i.$$

Thus R is not commutative.
The inverse of 2 in the quaternions is $1/2$. As this is not an element of R, R is not a division ring.
8. (i) 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.
(ii) 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 $H = \langle -1 \rangle$.
(iii) 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 $\langle -1 \rangle$.
(iv) 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.
9. 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

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

10. (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; an $n \times n$ matrix A has non-zero determinant iff it 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 2×2 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. If a, b and d are non-zero then there is a unique c such that

$$ad = bc \qquad \text{namely} \qquad c = \frac{ad}{b}.$$

Thus there are $(p-1)^3$ solutions of this form.
Otherwise one side of the equation is zero, so that the other side is zero as well. Thus we need to count the number of solutions of

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

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 $p^4 - (p-1)^3 - (2p-1)^2$ 2×2 matrices, with entries in $\mathbb{F}_p$.
One can check that the two methods to count the invertible matrices give the same answers.
(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.
By question (2), $b = c = 0$. Thus the only matrices which commute with every matrix must have the form

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

Take

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

Then

$$AB = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$$

but

$$AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$$

Thus if $AB = BA$ we must have $a = b$. Thus

$$A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI_2,$$

is a multiple of the identity.
On the other hand if $A = aI_2$ is a multiple of the identity and B is any matrix then

$$AB = (aI_2)B = a(I_2B) = aB \qquad \text{and} \qquad BA = B(aI_2) = a(BI_2) = aB.$$

Thus the centre of G consists of all non-zero multiples of the identity matrix.
(d) The order of G is $p(p-1)^2(p+1)$. Thus a Sylow-p subgroup P has order p. The centre has order $p-1$ so no subgroup of the centre will work and the only multiple of the identity in P must be I itself.
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.
11. 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 $b = c$.
12. Let R be a finite domain. It suffices to prove that every non-zero element a has an inverse. Define a map

$$f\colon R \longrightarrow R$$

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.

13. (i) 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 $na = [n]1$. 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. Pick a prime r that divides q. Then by Sylow's Theorems there is a subgroup R of order r of the additive group. Any non-zero element of R must have order r but it must also have order p by part (a). Thus $p = r$ and q is a power of p.