Groups and Rings III 2009

Assignment 5.

- Please hand up solutions to the starred questions by the 9.00am lecture on Wednesday 27th May. Either in the lecture or if earlier under the door of my office.
- Please try the unstarred questions by the tutorial on Wednesday 20th May at 9.00 at which they will be discussed.

1*. Find all groups of order 91.

2*. (a) Show that no group of order 40 is simple.
(b) Is there a finite group with 12 Sylow 3-subgroups? Give reasons for your answer.

3. Show that $G$ is a $p$-group (i.e has order a power of the prime $p$) if and only if every element of $G$ has order a power of $p$. (Hint: Cauchy's theorem)

4. Show that no group of order 1000 is simple.

5. Find all groups of order 133.

6*. Consider the ring of real quaternions:
$$\mathbb{R}(i) = \{x_1 + x_2 i + x_3 j + x_4 k \mid x_1, x_2, x_3, x_4 \in \mathbb{R}\}$$

We define the addition and multiplication by assuming everything is linear over the real numbers and using the usual rules of multiplications in the quaternion group. E.g. $(5 + 2j)(i + 3k) = 5i + 15k + 2ji + 2jk = (5 + 2)i + (15 - 2)k = 7i + 13k$ and $(1 + 3j) + (7i + 2j + k) = 1 + 7i + 5j + k$.

(a) If $x = x_1 + x_2 i + x_3 j + x_4 k$ define $\bar{x} = x_1 - x_2 i - x_3 j - x_4 k$ and show that $x \bar{x} = \|x\|^2$ where $\|x\|$ is the usual Euclidean length of a vector $(x_1, x_2, x_3, x_4) \in \mathbb{R}^4$.

(b) Deduce that any non-zero $x \in \mathbb{R}(i)$ is a unit.
(c) Deduce that $\mathbb{R}(i)$ is a skew-field.

7. Consider the set $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\} \subset \mathbb{Q}$.

(a) Show that $\mathbb{Q}(\sqrt{5})$ is a subring of $\mathbb{Q}$.
(b) Show that $\mathbb{Q}(\sqrt{5})$ is a field.

8*. Complete the following table.

<table>
<thead>
<tr>
<th>Ring</th>
<th>Commutative</th>
<th>Identity</th>
<th>Units</th>
<th>Zero Divers</th>
<th>Field</th>
<th>Integral Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$</td>
<td>yes</td>
<td>1</td>
<td>±1</td>
<td>none</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>$\mathbb{Z}(i)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\mathbb{Z}_8$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\mathbb{Z}_5$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\mathbb{Q}(\sqrt{3})$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\mathbb{R}(i)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$M_2(\mathbb{R})$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Note:
\( \mathbb{Z}(i) = \{ a + bi \mid a, b \in \mathbb{Z} \} \) is the ring of Gaussian Integers, a subring of \( \mathbb{C} \).
\( \mathbb{Q}(\sqrt{3}) = \{ a + b\sqrt{3} \mid a, b \in \mathbb{Q} \} \) is a subring of \( \mathbb{R} \).
\( \mathbb{R}(\mathbb{R}) \) see Question 6.
You don’t have to prove everything. Just fill out the table.

9*. Let \( D \) be a finite integral domain.

(a) Show that left cancellation holds in \( D \). That is if \( 0 \neq x \in D \) and \( xa = xb \) then \( a = b \).

(b) Let \( 0 \neq x \in D \) and consider the map \( \phi_x : D \to D \) defined by \( \phi_x(a) = xa \). Show that \( \phi_x \) is one to one and onto. (Hint: Recall that if \( X \) is a finite set and \( f : X \to X \) is one to one then \( f \) is onto.)

(c) Deduce that \( D \) is a field.

10. Recall the construction in lectures of the field of quotients of an integral domain \( D \) which involved the set \( S = \{(a,b) \mid a, b \in D, b \neq 0 \} \).

(a) Show that the relation \( (a,b) \sim (c,d) \) if \( ad = bc \) is an equivalence relation on \( S \).

(b) Show that the addition
\[
[(a,b)] + [(c,d)] = [(ad + bc, bd)]
\]
is well-defined.

11*. Let \( R \) be a ring with identity 1. Recall that for any positive integer \( n \) and element \( a \in R \)
\[
n.a = a + a + \ldots + a \quad \text{n times}
\]
The characteristic of \( R \) is the smallest positive integer \( n \) such that \( n.1 = 0 \), if such an \( n \) exists; otherwise \( R \) has characteristic 0.

(a) Show that if \( R \) has characteristic \( n \) then \( n.a = 0 \) for all \( a \in R \).

(b) If \( R \) is an integral domain with characteristic \( n \) \((n \neq 0)\) show that \( n \) is prime.

(c) (i) Deduce that every finite field \( F \) has characteristic \( p \), for some prime \( p \).

(ii) Further, show that \( |F| = p^m \) for some positive integer \( m \).

(Hint: Consider the group \( (F, +) \).)

12. If \( R \) is a ring a non-zero element is called a left zero-divisor if there is some non-zero \( b \) such that \( ab = 0 \) and similarly it is called a right zero-divisor if there is some non-zero \( b \) such that \( ba = 0 \).

(a) In the ring \( M_n(\mathbb{R}) \) of real matrices show that \( A \) is a left zero-divisor if and only if it has non zero kernel.

(b) In the same ring show that \( B \) is a right zero-divisor if and only if it has image not equal to all of \( \mathbb{R}^n \).

(c) Deduce that in \( M_n(\mathbb{R}) \) left and right zero-divisors are the same thing.

(d) Denote by \( \mathbb{R}^\infty \) the vector space of all infinite sequences of real numbers \((x_1, x_2, x_3, \ldots)\). Let \( M_\infty(\mathbb{R}) \) be the ring of all linear maps from \( \mathbb{R}^\infty \) to itself. Find a left zero divisor in \( M_\infty(\mathbb{R}) \) which is not a right zero divisor.

(Hint: For (b) and (c) remember that if \( W \) is a subspace of \( \mathbb{R}^n \) there is always a linear map \( P : \mathbb{R}^n \to \mathbb{R}^n \) with image \( W \) and a linear map \( Q \) with kernel \( W \). For example \( P \) could be orthogonal projection onto \( W \) and \( Q \) orthogonal projection onto \( W^\perp \). (d) could be tricky. Ask me if you want a hint.)