SECOND PRACTICE MIDTERM  
MATH 18.703, MIT, SPRING 13

You have 80 minutes. This test is closed book, closed notes, no calculators.

There are 6 problems, and the total number of points is 100. Show all your work. Please make your work as clear and easy to follow as possible. Points will be awarded on the basis of neatness, the use of complete sentences and the correct presentation of a logical argument.

Name:______________________________

Signature:___________________________

Student ID #:_______________________

<table>
<thead>
<tr>
<th>Problem</th>
<th>Points</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Presentation</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>
1. (15pts) (i) Give the definition of an irreducible element of an integral domain.

*Solution:* Let $R$ be an integral domain. We say that $a \in R$ is irreducible if whenever $a = bc$ then either $b$ or $c$ is a unit.

(ii) Give the definition of a prime element of an integral domain.

*Solution:* Let $R$ be an integral domain. We say that $p \in R$ is prime if the ideal $\langle p \rangle$ is a prime ideal, not equal to either $\{0\}$ or $R$.

(iii) Give the definition of a principal ideal domain.

*Solution:* Let $R$ be an integral domain. We say that $R$ is a principal ideal domain if every ideal is principal.
2. (15pts) (i) State the Sylow Theorems.

Solution: Let $G$ be a group of order $n$ and let $p$ be a prime dividing $n$.
Then the number of Sylow $p$-subgroups is equal to one modulo $p$, divides $n$ and any two Sylow $p$-subgroups are conjugate.

(ii) Prove that there is no simple group of order 120.

Solution: 120 = $2^3 \cdot 3 \cdot 5$. Then the number $n_5$ of Sylow 5-subgroups is congruent to one modulo 5 and divides $2^3 \cdot 3$. By the first condition

$$n_5 = 1, 6, 11, 16, 21$$

so that either $n_5 = 1$ or $n_5 = 6$. If $n_5 = 1$ then there is a unique Sylow 5-subgroup $P$ and this subgroup must be normal. If $n_5 = 6$ then there is a nontrivial action of $G$ on the set of Sylow 5-subgroups and so there is a representation

$$\rho: G \rightarrow S_6.$$ 

If $\rho$ is not injective then the kernel is a normal subgroup. If $\rho$ is injective then $G$ is isomorphic to a subgroup of $S_6$. Consider $H = A_6 \cap G \subset G$. If $G$ is not contained in $A_6$ then $H$ is a subgroup of index 2, in which case it is normal. So we may assume that $G$ is a subgroup of $A_6$ of index 3. The action of $A_6$ on the left cosets $G$ in $A_6$ defines a non-trivial representation

$$\rho: A_6 \rightarrow S_3,$$

whose kernel is a non-trivial normal subgroup of $A_6$, which contradicts the fact that $A_6$ is simple.
3. (15pts) Let $R$ be an integral domain and let $I$ be an ideal. Show that $R/I$ is a field iff $I$ is a maximal ideal.

Solution: We first show that if $R$ is an integral domain then $R$ is a field if and only if $\{0\}$ and $R$ are the only ideals.

Suppose that $R$ is a field. If $I \neq \{0\}$ is an ideal then pick $a \neq 0 \in I$. As $R$ is a field we may find $b \in R$ such that $ba = 1$. But then $1 \in I$ so that $I = R$. Thus $\{0\}$ and $R$ are the only ideals.

Now suppose that $\{0\}$ and $R$ are the only ideals. Pick $a \neq 0 \in R$. Then $I = \langle a \rangle$ is a non-zero ideal. It follows that $I = R$ and so $1 \in I$. But then we may find $b \in R$ such that $1 = ba$. Thus $a$ has an inverse and $R$ is a field.

Now suppose that $I$ is an ideal. Then there is a correspondence between ideals $J \trianglelefteq R$ which contain $I$ and ideals $I'$ in the quotient ring $R/I$; given $J$ let $I' = J/I$ be the image and given $I'$, let $J$ be the inverse image, under the natural map $R \rightarrow R/I$.

Then $R/I$ is a field if and only if $I' = \{0\}$ and $I' = R/I$ are the only ideals if and only if $J = I$ and $J = R$ are the only ideals containing $I$ if and only if $I$ is maximal.
4. (15pts) Let $R$ be a ring.

(i) If 

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n \subset \cdots,$$

is an ascending sequence of ideals then the union $I$ is an ideal.

\textit{Solution:} Suppose that $a$ and $b \in I$. Then $a \in I_m$ and $b \in I_n$ some $m$ and $n$. Let $k = \max(m, n)$. Then $a$ and $b \in I_k$ so that $a + b \in I_k \subset I$. Thus $I$ is closed under addition.

Now suppose that $a \in I$ and $r \in R$. Then $a \in I_m$ some $m$ and $ra \in I_m \subset I$, so that $I$ is an ideal.

(ii) Show that if $R$ is a PID then every ascending chain condition of ideals eventually stabilises.

\textit{Solution:} By assumption $I = \langle a \rangle$ for some $a \in I$. But then $a \in I_m$, some $m$. Let $n \geq m$. Then

$$\langle a \rangle \subset I_m \subset I_n \subset I = \langle a \rangle.$$

It follows that $I_n = \langle a \rangle$, so that the sequence above stabilises.
5. (20pts) Let $R$ be a ring and let $I$ and $J$ be two ideals.
(i) Show that the intersection $I \cap J$ is an ideal.

\textit{Solution:} Suppose that $a$ and $b \in I \cap J$. Then $a, b \in I$ so that $a + b \in I$. Similarly $a + b \in J$. But then $a + b \in I \cap J$ so that $I \cap J$ is closed under addition.
Now suppose that $a \in I \cap J$ and $r \in R$. Then $a \in I$ and so $ra \in I$. Similarly $ra \in J$. But then $ra \in I \cap J$ and so $I \cap J$ is an ideal.

(ii) Is the union $I \cup J$ an ideal?

\textit{Solution:} No. Let $R = \mathbb{Z}$, $I = \langle 2 \rangle$ and $J = \langle 3 \rangle$, the multiples of 2 and 3. Then $2 \in I \subset I \cup J$ and $3 \in J \subset I \cup J$ but $5 = 2 + 3 \notin I$ and $5 = 2 + 3 \notin J$ so that $I \cup J$ is not closed under addition.
6. (15pts) Let $R$ be a principal ideal domain and let $a$ and $b$ be two non-zero elements of $R$. Show that the gcd $d$ of $a$ and $b$ exists and prove that there are elements $r$ and $s$ of $R$ such that
\[ d = ra + sb. \]

Solution:
As $R$ is a PID, there is an element $d$ of $R$ such that
\[ \langle a, b \rangle = \langle d \rangle. \]
As $a \in \langle a, b \rangle = \langle d \rangle$, $d | a$. Similarly $d | b$. Suppose that $d' | a$ and $d' | b$. Then $a \in \langle d' \rangle$ and $b \in \langle d' \rangle$, so that
\[ \langle d \rangle \langle a, b \rangle \subset \langle d' \rangle. \]
But then $d' | d$ so that $d$ is the gcd.
Since $d \in \langle d \rangle = \langle a, b \rangle$, there are elements $r$ and $s$ of $R$ such that
\[ d = ra + sb. \]