SECOND MIDTERM
MATH 100B, UCSD, WINTER 16

You have 50 minutes.

There are 6 problems, and the total number of points is 85. Show all your work. *Please make your work as clear and easy to follow as possible.*

<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>10</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>10</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>85</td>
<td></td>
</tr>
</tbody>
</table>

Name: ________________________________

Signature: __________________________
1. (15pts) Give the definition of a prime element of a ring. A non-zero element $p$ of an integral domain $R$ is a prime if $\langle p \rangle$ is a prime ideal, not equal to the whole of $R$.

(ii) Give the definition of a unique factorisation domain. An integral domain $R$ is a UFD if every non-zero element, not a unit, is a product of primes and this factorisation is unique up to associates and re-ordering.

(iii) Give the definition of the gcd of a pair of elements of an integral domain. The gcd of two elements $a$ and $b$ is an element $d \in R$ such that $d|a$, $d|b$ and if $d'|a$ and $d'|b$ then $d'|d$. 

\[ \]
2. (15pts) (i) Let \( p \) and \( q \) be two primes in an integral domain \( R \). Show that if \( p \) divides \( q \) then \( p \) and \( q \) are associates. By assumption we may write \( q = ap \) for some \( a \in R \). As \( q \) is a prime, either \( q \) divides \( a \) or it divides \( p \). If it divides \( a \) then \( a = bq \) for some \( b \in R \). Therefore \( q = ap = bqp \) and so, cancelling, we must have \( 1 = bp \). But then \( p \) is a unit, a contradiction. Otherwise \( q \) divides \( p \) and so \( p \) and \( q \) are associates.

(ii) Suppose that \( p_1p_2 \ldots p_k = q_1q_2 \ldots q_l \), where \( p_1, p_2, \ldots, p_k \) and \( q_1, q_2, \ldots, q_l \) are primes. Show that \( k = l \) and that if we re-order \( q_1, q_2, \ldots, q_l \) then \( p_i \) and \( q_i \) are associates, for \( 1 \leq i \leq k \).

Since \( p_1 \) divides \( p_1p_2 \ldots p_k \) it must divide \( q_1q_2 \ldots q_l \). Thus \( p_1 \) must divide one of the factors. Re-ordering we may assume that \( p_1 \) divides \( q_1 \). Thus \( p_1 \) and \( q_1 \) are associates. Dividing both sides by \( p_1 \) we are done by induction on \( k \).
3. (10pts) Show that the set of all ideals satisfies the ascending chain condition in a principal ideal domain.

Let

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

be an ascending sequence of ideals. Let $I$ be the union. We check that $I$ is an ideal.

If $a$ and $b \in I$ then we may find $m$ and $n$ such that $a \in I_m$ and $b \in I_n$. Then $a$ and $b \in I_k$, where $k = \max(m, n)$. It follows that $a + b \in I_k$ so that $a + b \in I$. Now suppose that $r \in R$. Then $ra \in I_m$ so that $ra \in I$. Thus $I$ is an ideal.

As $R$ is a PID we may find $a \in R$ such that $I = \langle a \rangle$. As $a \in I$ it follows that $a \in I_m$, some $m$. But then

$$I = \langle a \rangle \subset I_n \subset I \quad \text{for all} \quad n \geq m.$$

Thus $I_n = I_m$ for all $n \neq m$. 
4. (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
\[ d = ra + sb. \]

Let $I = \langle a, b \rangle$. As $R$ is a PID, $I = \langle d \rangle$, for some $d \in R$. As $d \in I = \langle a, b \rangle$, there are $r$ and $s \in R$, such that $d = ra + sb$. It remains to prove that $d$ is the gcd.

As $a \in I = \langle d \rangle$, $d$ divides $a$. Similarly $d$ divides $b$. Thus $d$ is a common divisor. Now suppose that $d'$ is also a common divisor of $a$ and $b$. Then $a, b \in \langle d' \rangle$. Thus $d \in I = \langle a, b \rangle \subset \langle d' \rangle$. Thus $d \in \langle d' \rangle$ and $d'$ divides $d$. Thus $d$ is a greatest common divisor.
5. (20pts) (i) Carefully state Gauss’ Lemma. Let $R$ be an integral domain and let $F$ be its field of fractions. Suppose that $f(x) \in R[x]$ and the content of $f(x)$ is one. Then $f$ is irreducible over $R$ if and only if it is irreducible over $F$.

(ii) Prove that the polynomial

$$f(x) = x^3 + 3x + 2$$

is an irreducible element of $\mathbb{Q}[x]$.

Suppose not. Then $f$ is reducible over $\mathbb{Z}$. As $f$ is a cubic and the content is one, it must have a linear factor. Suppose that

$$x^3 + 3x + 2 = (x + a)(x^2 + bx + c),$$

where $a$, $b$ and $c$ are integers. Then $ac = 2$, so that $a = \pm 1, \pm 2$. But then $\pm 1, \pm 2$ would be a root of $f$, which it is easy to check is not the case.
6. (10pts) **State Eisenstein’s criteria.** Prove that the polynomial $f(x)$

$$6x^{13} - 21x^{12} + 35x^{11} + 42x^{10} - 56x^9 + 14x^8 + 21x^7 - 7x^6 - 42x^5 + 14x^4 + 21x^3 - 7x^2 + 28x + 7,$$

is an irreducible element of $\mathbb{Q}[x]$.

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial. Suppose that there is a prime $p$ which does not divide the leading coefficient of $f$, whilst it does divide the other coefficients, and such that $p^2$ does not divide the constant coefficient. Then $f$ is irreducible over $\mathbb{Q}$.

Apply Eisenstein with $p = 7$. 


Bonus Challenge Problems

7. (10pts) Let $p$ be a prime. Prove that

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

is irreducible over $\mathbb{Q}$.

See (10.17).
8. (10pts) Prove that if $I_1, I_2, \ldots, I_k$ are pairwise coprime ideals in a commutative ring $R$ and the product is the zero ideal, then $R$ is isomorphic to $\bigoplus_{i=1}^{k} R_i$, where $R_i = R/I_i$.

See Homework set 5.