Math 403, Jeffrey Adams  
Test II, April 30, 2010 Take Home SOLUTIONS

1. Suppose $R$ has no zero-divisors, and $a \in R$ $(a \neq 0)$ satisfies $a^2 = a$. Show that $a$ is a unity for $R$.

For $b \in R$ we have $a^2b = ab$, which can be written $(ab)a = ba$, or $(ab-b)a = 0$. Since there are no zero-divisors this implies $ab-b = 0$, or $ab = b$. This holds for all $a$: $a$ is a unity.

Note: If you assume $R$ has a unity 1, then $a^2 = a$ implies $a(a-1) = 0$, which implies $a = 1$ since there are no zero-divisors. But strictly speaking one shouldn’t assume there is a 1 beforehand.

2. Suppose $R$ is commutative with prime characteristic $p$.

(a) Show that for all $a, b \in R$, $(a+b)^p = a^p + b^p$.

By the binomial theory $(a+b)^p = \sum \binom{p}{k}a^kb^{p-k}$. It is a standard fact that $p$ divides $\binom{p}{k}$ for all $1 \leq k \leq p-1$. For example $\binom{p}{2} = p$, $\binom{p}{2} = p(p-1)/2$, etc. So reducing (mod $p$) all terms are 0 except the first and last, giving $a^p + b^p$

(b) Show that the map $f(a) = a^p$ is a ring homomorphism from $R$ to $R$. Obviously $f(ab) = (ab)^p = a^pb^p = f(a)f(b)$. Also $f(a+b) = (a+b)^p = a^p + b^p$ by part (a), and this equals $f(a) + f(b)$.

3. Suppose $R$ is commutative with unity. Let $S = \{ r \in R \mid r$ is not a unit $\}$. If $S$ is an ideal, show that it is (a) a maximal ideal in $R$, and (b) the unique maximal ideal.

Suppose $I \subset J \subset R$ and $I \neq J$. Then there is an element $a \in J - I$. By definition of $I$ $a$ is a unit (i.e. not a non-unit). But then $J = R$ as usual: for any $r$, $(ra^{-1})a = r \in J$.

For (b), if $I$ is a proper ideal then $I$ cannot contain a unit (which forces $I = R$). Therefore $I$ is contained in the non-units, i.e. $I \subset S$. So every proper ideal is contained in $S$, and $S$ is the unique maximal ideal.

4. Suppose $R, S$ are commutative with unities. Let $f$ be a homomorphism from $R$ onto $S$. Suppose $I$ is an ideal in $S$, and let $J = \{ r \in R \mid f(r) \in I \}$.

(a) Show that $J$ is an ideal in $R$.

This is straightforward. If $a, b \in J$, then $f(ab) = f(a)f(b)i$$I$, and $f(a) + f(b) \in I$, so $ab \in J, a + b \in J$. Also if $a \in R, b \in J$ then $f(ab) = f(a)f(b) \in I$ since $f(b) \in I$ and $I$ is an ideal. So $ab \in J$.

(b) If $I$ is prime show that $J$ is prime.

(c) If $I$ is maximal show that $J$ is maximal.

Consider the homomorphism $\phi : R \to S/I$, obtained by composing $f$ with the projection to $S/I$. This is surjective since $f$ is surjective. Its kernel is $J$: if $f(x) = 0$ in $S/I$, then $f(x) \in I$, i.e.
Recall $I$ is prime if and only if $R/I$ is an integral domain. By the isomorphism this holds if and only if $S/J$ is an integral domain, i.e. if and only if $J$ is prime.

Similarly with maximal in place of prime, and field in place of integral domain.

For another proof of (c), suppose $J \subset K \subset R$. We want to show $K = J$ or $K = R$. We have $I = f(J) \subset f(K) \subset S = f(R)$, and $f(K)$ is an ideal. Since $I$ is maximal, $I = f(K)$ or $S = f(K)$. If $I = f(K)$ then $K$ is contained in $f^{-1}(I) = J$, so $K = J$.

On the other hand suppose $f(K) = S$. This does not immediately imply $K = S$. Since $f(K) = S$ we can find $k \in K$ so that $f(k) = 1$. If $k = 1$ then $K = R$ and we’re done. But we can’t assume $f(k) = 1$. However $f(1) = 1$ also, so $f(k - 1) = f(k) - f(1) = 1 - 1 = 0$. Since $0 \in I$, this says $f(k - 1) \in I$, so $k - 1 \in J$. Write $k - 1 = j$ for some $j \in J$. Then $1 = k - j$. Since $k \in K, j \in J \subset K$, this says $1 \in K$, so indeed $K = R$.

5. Suppose $R$ is commutative and $I$ is a prime ideal of $R$. Show that (a) $I[x]$ is an ideal in $R[x]$ and (b) $I[x]$ is a prime ideal.

(a) If $p(x) = \sum a_i x^i \in R[x]$ and $f(x) = \sum b_j x^j \in I[x]$ then $f(x)p(x) = \sum_{i,j} a_i b_j x^{i+j}$. Since $b_j \in I, a_i \in R$ and $I$ is an ideal each $a_i b_j \in I$, so $f(x)p(x) \in I[x]$. Also clearly $I[x]$ is a ring.

(b) Suppose $f(x) = \sum a_i x^i \in R[x]$ and $g(x) = \sum b_j x^j \in R[x]$ and $f(x)g(x) \in I[x]$. We want to show all $a_i \in I$ or all $b_j \in I$.

Proof by contradiction: suppose not, and choose $r, s$ minimal so that $a_r \notin I, b_s \notin I$. The coefficient $c_{r+s}$ of $x^{r+s}$ in $f(x)g(x)$ is $c_{r+s} = \sum_{i+j=r+s} a_i b_j$. If $i + j = r + s$ then, unless $i = r, j = s$, either $i < r$ or $j < s$. By assumption $i < r$ implies $a_i \in$, and $j < s$ implies $b_j \in I$. Since $I$ is an ideal all terms in this sum are in $I$, except possibly $a_r b_s$. By assumption $c_{r+s} \in I$. Therefore $a_r b_s = c_{r+s} - \sum a_i b_j$ where the sum is over all $i + j = r + s$ except $i = r, j = s$. All terms on the right are on $I$, so $a_r b_s \in I$, a contradiction.

Here is another nice proof, provided by someone in class. There is a natural homomorphism $\psi : R[x]/I[x] \rightarrow (R/I)[x]$. Since $I$ is prime $R/I$ is an integral domain, and by Theorem 16.1 $(R/I)[x]$ is an integral domain. Now it is not hard to see $\psi$ is an isomorphism. So $R[x]/I[x]$ is an integral domain, which implies $I[x]$ is prime.
6. For $p$ a prime determine the number of irreducible polynomials over $\mathbb{Z}_p$ of degree 2.

The polynomials $(x - a)(x - b)$ are reducible. There are $\binom{p}{2}$ with $a \neq b$, and $p$ with $a = b$, for a total of $p + \binom{p}{2} = p(p + 1)/2$. These are the ones with coefficient of $x^2$ equal to 1. Multiply by $p - 1$ to have arbitrary such coefficient. There are thus $(p - 1)p(p + 1)/2$ reducible polynomials. There are $(p - 1)p^2$ polynomials of degree 2, so there are $(p - 1)p^2 - (p - 1)p(p + 1)/2 = (p - 1)\binom{p}{2}$ irreducible ones.