Homework #12, due 12/2/09 = **7.3.16**, **7.3.34**, **7.3.35**, **7.4.5**, **7.4.7**, **7.4.11**, **7.4.19**

7.3.16 Let $\varphi : R \to S$ be a surjective homomorphism of rings. Prove that the image of the center of R is contained in the center of S (cf. Exercise 7 of Section 7.1).

Suppose $c \in R$ is in the center of R. This means $cr = rc$ for every $r \in R$. We wish to show that $\varphi(c)$ is in the center of S.

Let $s \in S$. Since φ is surjective, there is some $r \in R$ such that $\varphi(r) = s$. Then $cr = rc$ since c is in the center of R, so $\varphi(cr) = \varphi(rc)$, but φ is a homomorphism, so $\varphi(c)\varphi(r) = \varphi(r)\varphi(c)$, but $\varphi(r) = s$, so $\varphi(c)s = s\varphi(c)$. Thus $\varphi(c)$ commutes with every $s \in S$, so $\varphi(c)$ is in the center of S.

7.3.34 Let I and J be ideals of R.

(a) Prove that $I + J$ is the smallest ideal of R containing both I and J.

First recall that $I + J = \{i + j | i \in I, j \in J\}$. Since $0 \in I \cap J$ we have $I = I + 0 \subseteq I + J$ and $J = J + 0 \subseteq I + J$, so $I + J$ does contain both I and J.

Next we show $I + J$ is an ideal. Consider two arbitrary elements $i_0 + j_0$ and $i_1 + j_1$ in $I + J$, where $i_0, i_1 \in I$ and $j_0, j_1 \in J$. Then $(i_0 + j_0) - (i_1 + j_1) = (i_0 - i_1) + (j_0 - j_1)$, but $i_0 - i_1 \in I$ and $j_0 - j_1 \in J$ since I and J are ideals, so $(i_0 + j_0) - (i_1 + j_1) \in I + J$. Thus $I + J$ is closed under differences. Consider an arbitrary element $i + j$ of $I + J$, where $i \in I$ and $j \in J$. Let $r \in R$. Then $ri, ir \in I$ and $rj, jr \in J$ since I and J are ideals. Then $r(i + j) = ri + rj = I + J$ and $(i + j)r = ir + jr \in I + J$. Thus $I + J$ is closed under left and right multiplication by arbitrary elements of R.

Finally, suppose K is an ideal of R containing both I and J. Consider an arbitrary element $i + j$ of $I + J$, where $i \in I$ and all $j \in J$. We have $i, j \in K$ since $I \cup J \subseteq K$, so $i + j \in K$ since K is closed under $+$. This shows $I + J \subseteq K$, so $I + J$ is the smallest ideal containing both I and J.

(b) Prove that IJ is an ideal contained in $I \cap J$.

Recall that IJ is the set of finite sums of products of the form ij with $i \in I$ and $j \in J$. Every such product is clearly in both I and J, since I and J are closed under multiplication by arbitrary elements of R. Since I and J are both closed under $+$, their intersection $I \cap J$ is also closed under $+$, so every sum of products of the form ij with $i \in I$ and $j \in J$ must also be in $I \cap J$. Therefore $IJ \subseteq I \cap J$.

To show IJ is an ideal, consider two arbitrary elements of IJ, say

$$i_1 j_1 + \cdots + i_m j_m,\ i'_1 j'_1 + \cdots + i'_n j'_n \in IJ$$

where

$$i_1, \cdots, i_m, i'_1, \cdots, i'_n \in I$$

and

$$j_1, \cdots, j_m, j_1', \cdots, j_n' \in J$$

Ideals are closed under differences and contain 0, so ideals are closed under additive inverse $-$, that is, if $i \in I$ then $-i = 0 - i \in I$. Thus $i_1, \cdots, i_m, -i_1', \cdots, -i_n' \in I$ and $j_1, \cdots, j_m, j_1', \cdots, j_n' \in J$, so the difference of two elements in IJ is again in IJ because it is a finite sum of products of the form ij ($i \in I$, $j \in J$):

$$\begin{aligned} &i_1j_1 + \cdots + i_mj_m - (i_1'j_1' + \cdots + i_n'j_n') \\ &= i_1j_1 + \cdots + i_mj_m + (-i_1')j_1' + \cdots (-i_n')j_n' \in IJ \end{aligned}$$

For any $r \in R$, we have $ri_1, \cdots, ri_m \in I$ since I is an ideal, $j_1r, \cdots, j_mr \in J$ since J is an ideal, and

$$\begin{aligned} r(i_1j_1 + \cdots + i_mj_m) &= (ri_1)j_1 + \cdots + (ri_m)j_m \in IJ \\ (i_1j_1 + \cdots + i_mj_m)r &= i_1(j_1r) + \cdots + i_m(j_mr) \in IJ \end{aligned}$$

So IJ is an ideal because it is closed under difference and also closed under left and right multiplication by arbitrary elements of R.

(c) Give an example where $IJ \neq I \cap J$.

Consider ideals in the ring $\mathbb{Z}$. For every $a \in \mathbb{Z}$, the ideal (a) generated by a is just the set of multiples of a. Obviously $(a^2) \subseteq (a)$, and $(a)(a) \subseteq (a^2)$ because $(a)(a)$ is the set of finite sums of products of two multiples of a, so it is the set of finite sums of multiples of a^2, each of which is a multiple of a^2:

$$\begin{aligned} &(x_1a)(y_1a) + \cdots + (x_na)(y_na) \\ &= x_1y_1a^2 + \cdots + x_ny_na^2 \\ &= (x_1y_1 + \cdots + x_ny_n)a^2 \in (a^2) \end{aligned}$$

Let $a > 0$ and $I = J = (a)$. Then $I \cap J = (a)$ and $IJ = (a)(a) = (a^2)$, so $IJ \neq I \cap J$ because $a \in (a)$ but $a \notin (a^2)$.

(d) Prove that if R is commutative and $I + J = R$ then $IJ = I \cap J$.

First we will give a counterexample. Let A be a nontrivial finite abelian group. Define a binary operation $\times$ on A by $a \times a' = 0$ for all $a, a' \in A$. Let R be the ring $(A, \times)$. (This is the first example of a ring in Section 7.1.) Let $R = I = J$. Then I and J are ideals of R, $I + J = R + R = R$, and $I \cap J = R \cap R = R$. However, $IJ = RR = \{0\}$, so $IJ \neq I \cap J$.

Next we prove **(d)** assuming R is not only a commutative ring, but also a ring with 1. Assume I and J are ideals of R such that $R = I + J$. We need only show $I \cap J \subseteq IJ$ since we always have $IJ \subseteq I \cap J$. Let $e \in I \cap J$. We have $1 \in R = I + J$ so $1 = i + j$ for some $i \in I$ and some $j \in J$. Then, since R is commutative, $e = e1 = e(i + j) = ei + ej = ie + ej$. However, $ie \in IJ$ (since $i \in I$ and $e \in J$) and $ej \in IJ$ (since $e \in I$ and $j \in J$). By the definition of IJ, this gives us $e \in IJ$. Thus $I \cap J \subseteq IJ$.

7.3.35 Let I, J, and K be ideals of R.

(a) Prove that $I(J+K) = IJ + IK$ and $(I+J)K = IK + JK$.

Consider an arbitrary element in $I(J+K)$, say

$$i_1(j_1 + k_1) + \cdots + i_n(j_n + k_n)$$

where $i_1, \cdots, i_n \in I$, $j_1, \cdots, j_n \in J$, and $k_1, \cdots, k_n \in K$. Then

$$\begin{aligned} &i_1(j_1 + k_1) + \cdots + i_n(j_n + k_n) \\ &= i_1 j_1 + i_1 k_1 + \cdots + i_n j_n + i_n k_n \\ &= i_1 j_1 + \cdots + i_n j_n + i_1 k_1 + \cdots + i_n k_n \in IJ + IK \end{aligned}$$

This shows one direction, that $I(J+K) \subseteq IJ + IK$.

For the other direction first note that $J \subseteq J + K$ and $K \subseteq J + K$ since $0 \in K$, so it follows by the definitions that $IJ \subseteq I(J+K)$ and $IK \subseteq I(J+K)$, which together imply

$$IJ + IK \subseteq I(J+K) + I(J+K). \tag{1}$$

Now J and K are ideals, so $J+K$ is also an ideal (the least ideal containing both J and K). But then, since I and $J+K$ are ideals, we conclude that $I(J+K)$ is also an ideal. Ideals are closed under $+$, so

$$I(J+K) + I(J+K) \subseteq I(J+K). \tag{2}$$

From (1) and (2) we get $IJ + IK \subseteq I(J+K)$.

The proof of $(I+J)K = IK + JK$ is essentially the same, involving left-right reversals, and I won't write it out here.

(b) Prove that if $J \subseteq I$ then $I \cap (J+K) = J + (I \cap K)$.

From the hypothesis $J \subseteq I$ and $J \subseteq J + K$ (since $0 \in K$) we get

$$J \subseteq I \cap (J+K) \tag{3}$$

From $I \cap K \subseteq I$ and $I \cap K \subseteq K \subseteq J + K$ (since $0 \in J$) we get

$$I \cap K \subseteq I \cap (J+K). \tag{4}$$

Now $I \cap (J+K)$ is an ideal and is closed under $+$, so

$$J + (I \cap K) \subseteq I \cap (J+K).$$

For the inclusion in the opposite direction, assume $i \in I \cap (J+K)$, so there are $j \in J$ and $k \in K$ such that $i = j + k$. Then $k = i - j$, but $j \in J \subseteq I$ and $i \in I$, so $k = i - j \in I$. Thus we have $k \in I \cap K$, so $i = j + k \in J + (I \cap K)$, as desired.

7.4.5 Let R be a ring, not necessarily commutative. Prove that if M is an ideal of R such that R/M is a field, then M is a maximal ideal.

Suppose I is an ideal of R such that $M \subset I \subset R$. We will prove that either $I = M$ or $I = R$, which shows that M must be maximal. By the Third Isomorphism Theorem, I/M is an ideal of R/M (and $(R/M)/(I/M) \cong$

R/I). But R/M is a field, so by Proposition 7.9, page 254, the only ideals of R/M are $\{M\}$ (the zero ideal of R/M) and R/M (the whole ring). Hence I/M is either the zero ideal $\{M\}$ of R/M, or else $I/M = R/M$. Thus we have either

$$\{M\} = I/M = \{i + M | i \in I\}$$

or else

$$R/M = I/M = \{i + M | i \in I\}.$$

If $\{M\} = \{i + M | i \in I\}$ then for every $i \in I$ we have $i + M = M$, hence $i \in M$. This shows $I \subseteq M$. But we already assumed $M \subseteq I$, so $I = M$. On the other hand, if $R/M = \{i + M | i \in I\}$, then for every $r \in R$ we have $r \in r + M \in \{r + M | r \in R\} = R/M = \{i + M | i \in I\}$, hence there is some $i \in I$ such that $r \in i + M$. But $i + M \subseteq I + M$, and $I + M \subseteq I$ since $M \subseteq I$, so $r \in I$. This shows that every element of R is in I, hence $I = R$.

7.4.7 Let R be a commtutative ring with 1. (1) Prove that the principal ideal generated by x in the polynomial ring $R[x]$ is a prime ideal if and only if R is an integral domain. (2) Prove that (x) is a maximal ideal if and only if R is a field.

We will use the fact, stated in the last two lines of page 252 and proved in class, that the ideal generated by a single element a iny commutative ring R consists of simply the multiples of that element, that is, $(a) = \{ra | r \in R\}$.

Proof of (1). Assume first that R is an integral domain. We wish to show that (x) is a prime ideal. Since (x) is an ideal of $R[x]$, we need only show that (x) is prime. Suppose $pq \in (x)$. We must show either p or q is in (x).

Note that $R[x]$ is commutative because R is commutative. Therefore, from the assumption $pq \in (x)$ and the fact stated above, we know pq must be a multiple of x, say $pq = ax$ for some $a \in R$. By Proposition 7.4(1), page 236, the sum of the degrees of p and q must be the degree of ax, which is 1. Hence the degrees of the polynomials p and q are either 1 and 0, respectively, or else 0 and 1, respectively. Suppose the former, say $p = bx + c$, $b, c \in R$, and $q \in R$. Then $ax = pq = (bx + c)q = bqx + cq$, so $a = bq$ and $0 = cq$. If c and q are both nonzero, then R contains zero divisors and is therefore not an integral domain, contrary to assumption. Therefore either $c = 0$ or $q = 0$. If $c = 0$ then $p = bx + c = px + 0 = px \in (x)$, as desired, so assume $c \neq 0$. Then $q = 0$, but $0 \in (x)$, so $q \in (x)$, as desired.

For the converse, assume (x) is prime. To show R is an integral domain, assume $r, s \in R$ and $rs = 0$. we wish to show either $r = 0$ or $s = 0$. Since (x) is an ideal, we have $0 \in (x)$, hence $rs \in (x)$. Since (x) is prime, either $r \in (x)$ or $s \in (x)$. Hence there are $a, b \in R$ such that either $r = ax$ or $s = bx$. But $r = ax$ really says $r + 0x = 0 + ax$, hence $r = 0$ and $a = 0$. Similarly, $s = bx$ implies $s = 0 = b$. But we know that either $r = ax$ or $s = bx$, so either $r = 0$ or $s = 0$, as desired.

Proof of (2): Assume (x) is a maximal ideal. Since $R[x]$ is commutative and has a 1, it follows by Proposition 7.12, page 255, that $R[x]/(x)$ is a field. This field happens to be isomorphic to R, so R is a field, but for a more direct argument, assume $0 \neq r \in R$. Then $(x) \neq r + (x)$ in $R[x]/(x)$, so $r + (x)$ has a multiplicative inverse in $R[x]/(x)$, say $s + (x)$, so that

$$1 + (x) = (r + (x))(s + (x)) = rs + (x)$$

hence $rs - 1 \in (x)$. But the degree of $rs - 1$ is 0, and the degree of every *nonzero* polynomial in (x) is 1 or more, so $rs - 1$ must be the zero polynomial. Thus $rs - 1 = 0$, so $rs = 1$ (and $sr = 1$ since R is commutative). This means that the arbitrary nonzero element r of R has a multiplicative inverse s, which shows R is a field.

For the converse of (2), assume R is a field. Let φ be the ring homomorphism that maps each polynomial $p(x) \in R[x]$ to its constant: $\varphi(r_0 + r_1x + \cdots r_nx^n) = r_0$. This homomorphism is discussed in example (5), page 245, where it is noted that φ is the homomorphism determined by evaluation at 0, that is, $\varphi(p(x)) = p(0)$. The kernel of φ is the set of polynomials in $R[x]$ whose constant is 0. But the multiples of x are the polynomials with constant 0, so the kernel of φ is simply (x). Clearly φ maps $R[x]$ onto R, so by the First Isomorphism Theorem, $R[x]/(x) \cong R$. Since the quotient is a field, it follows from Proposition 7.12, page 255, that (x) is maximal.

7.4.11 Assume R is commutative. Let I and J be ideals of R and assume P is a prime ideal of R that contains IJ (for example, if P contains $I \cap J$). Prove that either I or J is contained in R.

If $I \subseteq P$ we are done, so let us assume that I is not contained in P. Then there must be some element $i \in I$ such that $i \notin P$. We will show that $J \subseteq P$. Let $j \in J$. Then $ij \in IJ \subseteq P$, but P is prime, so either $i \in P$ or $j \in P$, but $i \notin P$, so $j \in P$. This proves $J \subseteq P$.

7.4.19 Let R be a finite commutative ring with identity. Prove that every prime ideal of R is a maximal ideal.

Let $P \subseteq R$ be a prime ideal. Then R/P is an integral domain by Proposition 7.13. R/P is finite because R is finiteso R/P is a finite integral domain. But then R/P is a field by Corollary 7.3, so P is a maximal ideal by Proposition 7.12.