Kris Harper
MATH 25800
Homework 2 January 22, 2010

Problem 1 (7.4.4)**.** *Assume R is commutative. Prove that R is a field if and only if 0 is a maximal ideal.*

Proof. Assume that R is a field. Then then only ideals are 0 and R. Since 0 is contained in no proper ideal other than itself, it must be maximal. Conversely, suppose 0 is a maximal ideal. We know that an ideal M is maximal if and only if R/M is a field. Thus $R/0 \cong R$ is a field. □

Problem 2 (7.4.5)**.** *Prove that if M is an ideal such that R/M is a field then M is a maximal ideal (do not assume R is commutative).*

Proof. Let R/M be a field and suppose to the contrary that M is not maximal so that there exists some ideal M' with $M \subsetneq M' \subsetneq R$. Let $\varphi : R/M \to R/M'$ be a function defined by $\varphi(r + M) = r + M'$. Then

$$\varphi((r + M) + (s + M)) = \varphi(r + s + M) = r + s + M' = (r + M') + (s + M') = \varphi(r + M) + \varphi(s + M)$$

and

$$\varphi((r + M)(s + M)) = \varphi(rs + M) = rs + M' = (r + M')(s + M') = \varphi(r + M)\varphi(s + M)$$

so φ is a homomorphism. Note that since M is strictly smaller than M', φ can't be injective. But this is a contradiction because R/M is a field and any homomorphism from a field to another ring must be an injection. Therefore M must be a maximal ideal. □

Problem 3 (7.4.7)**.** *Let R be a commutative ring with 1. Prove that the principle ideal generated by x in the polynomial ring $R[x]$ is a prime ideal if and only if R is an integral domain. Prove that (x) is a maximal ideal if and only if R is a field.*

Proof. We know that (x) is a prime ideal if an only if $R[x]/(x)$ is an integral domain. The problem is then reduced to showing $R[x]/(x) \cong R$. Let $\varphi : R[x]/(x) \to R$ be the function which takes $p(x)+(x) \in R[x]$ to the constant term of $p(x)$. It's clear that φ is a ring homomorphism since adding and multiplying two polynomials will add or multiply their constant terms respectively. Let $p(x) = r_n x^n + \cdots + r_0$ and $q(x) = s_n x^n + \cdots + s_0$. Then

$$p(x) + (x) = r_n x^n + \cdots + r_0 + (x) = (r_n x^n + (x)) + \cdots + (r_0 + (x)) = 0 + \cdots + r_0 + (x).$$

In the same way, $q(x) + (x) = s_0 + (x)$ and we see that two elements of $R[x]/(x)$ are equal precisely when their constant terms are the same. Thus, if we assume $p(x) \neq q(x)$, then $r_0 \neq s_0$ and $\varphi(p(x) + (x)) = r_0 \neq s_0 = \varphi(q(x) + (x))$. Therefore, φ is injective. It's clear that φ is surjective since φ applied to a constant is just the identity function. Thus, φ is a bijection from $R[x]/(x)$ to R so $R[x]/(x) \cong R$. Therefore (x) is a prime ideal if and only if R is an integral domain.

As before, we know that (x) is a maximal ideal if and only if $R[x]/(x)$ is a field. But we've just shown that $R[x]/(x) \cong R$ so (x) is a maximal ideal if and only if R is a field. □

Problem 4 (7.4.10)**.** *Assume R is commutative. Prove that if P is a prime ideal of R and P contains no zero divisors then R is an integral domain.*

Proof. Let $a, b \in R$ be two elements such that $ab = 0$. Since P is an ideal, $0 \in P$ and so either $a \in P$ or $b \in P$. But since P contains no zero divisors, we must have $a = 0$ or $b = 0$. Thus R is an integral domain. □

Problem 5 (7.4.13)**.** *Let $\varphi : R \to S$ be a homomorphism of commutative rings.*
(a) Prove that if P is a prime ideal of S then either $\varphi^{-1}(P) = R$ or $\varphi^{-1}(P)$ is a prime ideal of R. Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if P is a prime idea of S then $P \cap R$ is either R or a prime ideal of R.
(b) Prove that if M is a maximal ideal of S and φ is surjective then $\varphi^{-1}(M)$ is a maximal ideal of R. Give an example to show that this need not be the case if φ is not surjective.

Proof. (a) Let P be a prime ideal of S. We've already shown that $\varphi^{-1}(I)$ is an ideal of R for any ideal I of S. It's possible that $\varphi^{-1}(P) = R$, in which case we're done, so assume otherwise. Now let $ab \in \varphi^{-1}(P)$. Then $\varphi(ab) \in P$ so $\varphi(a)\varphi(b) \in P$. Since P is prime, either $\varphi(a) \in P$ or $\varphi(b) \in P$, which means either $a \in \varphi^{-1}(P)$ or $b \in \varphi^{-1}(P)$. Thus $\varphi^{-1}(P)$ is prime.

In the special case that φ is an inclusion homomorphism, φ is the identity on R, so $\varphi^{-1}(P)$ consists of elements of R which are also elements of P. That is, $\varphi^{-1}(P) = P \cap R$ and by the above proof, we know this is now either R itself, or a prime ideal of R.

(b) Let M be a maximal ideal of S and suppose that φ is surjective. We know that $\varphi^{-1} \neq R$ since $M \neq S$ and φ is surjective. Suppose there exists some ideal M' such that $\varphi^{-1}(M) \subseteq M' \subseteq R$. Since φ is surjective, $\varphi(M')$ is an ideal of S and $M \subseteq \varphi(M')$. Since M is maximal, we either have $M = \varphi(M')$ or $\varphi(M') = S$. Suppose the former and let $x \in M'$. Then $\varphi(x) \in \varphi(M')$ so $\varphi(x) \in M$. Then $x \in \varphi^{-1}(M)$ and we have $M' \subseteq \varphi^{-1}(M)$. This shows $M' = \varphi^{-1}(M)$. Secondly, suppose $\varphi(M') = S$ and let $x \in R$. Then $\varphi(x) \in S$ and $\varphi(x) \in \varphi(M')$. Thus there exists $y \in M'$ such that $\varphi(x) = \varphi(y)$. Then we have $\varphi(x) - \varphi(y) = \varphi(x - y) = 0$ so $x - y \in \ker\varphi$. Note that $\ker\varphi = \varphi^{-1}(0) \subseteq M'$. Therefore $x = y + (x - y)$ is in M' which shows $R \subseteq M'$ and $R = M'$. In all cases we either have $M' = \varphi^{-1}(M)$ or $M' = R$ so $\varphi^{-1}(M)$ is maximal in R. ☐

Problem 6 (7.4.16)**.** *Let $x^4 - 16$ be an element of the polynomial ring $E = \mathbb{Z}[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{Z}[x]/(x^4 - 16)$.*
(a) Find a polynomial of degree ≤ 3 that is congruent to $7x^{13} - 11x^9 + 5x^5 - 2x^3 + 3$ modulo $(x^4 - 16)$.
(b) Prove that $\overline{x-2}$ and $\overline{x+2}$ are zero divisors in $\overline{E}$.

Proof. (a) We need to find a polynomial with degree less than or equal to 3 which has the same remainder as $7x^{13} - 11x^9 + 5x^5 - 2x^3 + 3$ when divided by $x^4 - 16$. Note that $(7x^{13} - 11x^9 + 5x^5 - 2x^3 + 3)/(x^4 - 16)$ has remainder $-2x^3 + 25936x + 3$. This remainder is then a polynomial which cannot be reduced by dividing by $x^4 - 16$ and so it serves as its own remainder. Thus $7x^{13} - 11x^9 + 5x^5 - 2x^3 + 3 \equiv -2x^3 + 25936x + 3 \pmod{x^4 - 16}$.

(b) Note that $x^4 - 16 = (x - 2)(x + 2)(x^2 + 4)$. Thus

$$(\overline{x-2})(\overline{x^3 + 2x^2 + 4x + 8}) = \overline{0}$$

and

$$(\overline{x+2})(\overline{x^3 - 2x^2 + 4x - 8}) = \overline{0}.$$

Since $x + 2$, $x - 2$, $x^3 - 2x^2 + 4x - 8$ and $x^3 + 2x^2 + 4x + 8$ all have degree less than or equal to three, they can't be equal to 0 in $\overline{E}$. Thus, they are all zero divisors. ☐

Problem 7 (7.4.17)**.** *Let $x^3 - 2x + 1$ be an element of the polynomial ring $E = \mathbb{Z}[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{Z}[x]/(x^3 - 2x + 1)$. Let $p(x) = 2x^7 - 7x^5 + 4x^3 - 9x + 1$ and let $q(x) = (x - 1)^4$.*
(a) Express each of the following elements of $\overline{E}$ in the form $\overline{f(x)}$ for some polynomial $f(x)$ of degree ≤ 2: $\overline{p(x)}$, $\overline{q(x)}$, $\overline{p(x) + q(x)}$ and $\overline{p(x)q(x)}$.
(b) Prove that $\overline{E}$ is not an integral domain.
(c) Prove that $\overline{x}$ is a unit in $\overline{E}$.

Proof. (a) As in part (a) of Problem 6, we note that $p(x)$ is congruent to it's remainder when divided by $x^3 - 2x + 1$ modulo $x^3 - 2x + 1$. If these remainders have degree less than or equal to 2, then we're done. Dividing and looking at the remainders gives the following equalities. We have $\overline{p(x)} = \overline{-x^2 - 11x + 3}$, $\overline{q(x)} = \overline{8x - 5}$, $\overline{p(x) + q(x)} = \overline{7x^2 - 24x + 8}$ and $\overline{p(x)q(x)} = \overline{146x - 90}$.

(b) We see that $x^3 - 2x + 1 = (x - 1)(x^2 + x - 1)$ and so $\overline{x - 1}$ is a zero divisor.

(c) Note that $\overline{x^3 - 2x} + \overline{1} = \overline{0}$ and so $\overline{1} = \overline{-x^3 + 2x}$. Thus $\overline{x}\overline{-x^2 + 2} = \overline{-x^3 + 2x} = \overline{1}$ and $\overline{x}$ is a unit. ☐

Problem 8 (7.6.3)**.** *Let R and S be rings with identities. Prove that every ideal of $R \times S$ is of the form $I \times J$ where I is an ideal of R and J is an ideal of S.*

Proof. Let K be an ideal of $R \times S$ and write $K \subseteq I \times J$ where I is the subset of R which makes up the left components of K and J is the subset of S which makes up the right components. Let $a, b \in I$ and $c, d \in J$ such that $(a, c), (b, d) \in K$. Note that $(a, c) - (b, d) = (a - b, c - d)$ so $a - b \in I$ and $(a, c)(b, d) = (ab, cd)$ so $ab \in I$. Furthermore, for $r \in R$ we have $(a, c)(r, c) = (ar, c^2)$ and $(r, c)(a, c) = (ra, c^2)$ so I is closed under left and right multiplication by elements of R. This shows that I is an ideal of R and similarly, that J is an ideal of S.

Finally, let (a, c) be an arbitrary element of $I \times J$. This means there exists some $(a, c') \in K$ and since K is closed under multiplication by elements from $R \times S$, we have $(a, c')(1, 0) = (a, 0)$ is an element of K as well. Similarly, $(0, c) \in K$. But now $(a, c) = (a, 0) + (0, c)$ and so $(a, c) \in K$ since K is closed under addition. Therefore $I \times J \subseteq K$ and $K = I \times J$ where I is an ideal of R and J is an ideal of S. $\square$