MATH 258: Homework #3

Jesse Farmer

26 January 2005

1. *Let R be a commutative ring. Prove that R is a field if and only if 0 is a maximal ideal.*

   Assume 0 is a maximal ideal. Then $R \cong R/\{0\}$ is a field. Conversely, assume R is a field and let I be an ideal of R containing a nonzero element a. Then $1 = a^{-1}a \in I$, and hence $I = R$. Therefore 0 is a maximal ideal.

2. *Let R be an integral domain. Prove that $(a) = (b)$ for some $a, b \in R$ if and only if there exists some unit $u \in R$ such that $a = ub$.*

   Recall that $(a) = \{ra \mid r \in R\}$. Assume $(a) = (b)$, then for any $r_1 \in R$ there exists an $r_2 \in R$ such that $r_1 a = r_2 b$. In particular, there exist $u, v \in R$ such that $a = ub$ and $va = b$. u is a unit since
   $$a = ub = u(va) = (uv)a$$
   and hence $uv = 1$ since R is an integral domain. Assume $a = ub$ for some unit u of R. $(a) \subset (b)$ since for any $ra \in (a)$, $ra = rub \in (b)$. Conversely, $b = u^{-1}a$, so that for any $rb \in (b)$, $rb = ru^{-1}b \in (a)$, and hence $(a) = (b)$.

3. *Let R be the ring of all continuous function on $[0, 1]$ and let I be the collection of functions $f \in R$ with $f(1/3) = f(1/2) = 0$. Prove that I is an ideal of R but is not a prime ideal.*

   Let $g \in R$ and $f \in I$, then, for $x = 1/2, 1/3$,
   $$(gf)(x) = g(x)f(x) = g(x)0 = 0$$
   Similarly, for $g, f \in I$ and $x = 1/2, 1/3$,
   $$(g + f)(x) = g(x) + f(x) = 0 + 0 = 0$$
   Therefore I is an ideal. To see that it is not a prime ideal, consider $f(x) = x - 1/3$ and $g(x) = x - 1/2$. Then neither f nor g is in I, but fg is.

4. *Let R be a commutative ring. Let I and J ideals of R, and P a prime ideal of R that contains IJ. Prove that either I or J is contained in P.*

   Assume for contradiction that neither I nor J is contained in P. Pick $a \in I$ and $b \in J$ not in P, then $ab \in IJ \subset P$. But since P is a prime ideal, one of a or b must be in P – a contradiction. Hence I or J must be contained in P.

5. *Let R be a commutative ring and suppose I and J are two finitely generated ideals of R. Prove that IJ is finitely generated.*

   Let A and B be finite subsets of R and $I = (A)$ and $J = (B)$. Let K be the ideal generated by all $a_i b_i$ with $a_i \in A$ and $b_i \in B$. Clearly $K \subset IJ$ since $A \subset (A)$ and $B \subset (B)$, so that if $x \in K$ then

   $$x = \sum_{i=1}^{l} r_i a_i b_i \in IJ$$

   since $r_i a_i \in (A)$ and $b_i \in B \subset (B)$. The other inclusion is equally obvious, though more tedious. It is sufficient to prove that $a'b' \in K$ for every $a' \in (A)$ and $b' \in (B)$ since every element in IJ is a sum of $a'b'$. So let $a' = \sum_{i=1}^{\infty} r_i a_i$ and $b' = \sum_{i=1}^{\infty} r_i' b_i$, where all but finitely many r_i and r_i' are zero. Then

   $$a'b' = \sum_{i=1}^{\infty} c_i$$

   where $c_i = \sum_{k=0}^{i} r_{k,i-k} a_k b_{i-k}$ and $r_{k,i-k} = r_i r_{i-k}'$. Then $c_i \in K$, and hence the sum of any number of c_i is in K since there are only finitely many nonzero c_i.

6. *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 where R is a subring of S and φ is the inclusion homomorphism to deduce that if P is a prime ideal of S then $P \cap R$ is either R or a prime ideal of R.*

   The preimage of a subgroup is itself a subgroup, so take $r \in R$ and $x \in \varphi^{-1}(P)$, then $\varphi(rx) = \varphi(r)\varphi(x) \in P$ since P is an ideal, and $rx \in \varphi^{-1}(P)$. Let $ab \in \varphi^{-1}(P)$, then $\varphi(a)\varphi(b) = \varphi(ab) \in P$, which means $\varphi(a) \in P$ or $\varphi(b) \in P$, i.e., $a \in \varphi^{-1}(P)$ or $b \in \varphi^{-1}(P)$. If P is a prime ideal then $1_S \notin P$, but that means $\varphi(1_R) \notin P$, i.e., $1_R \notin \varphi(P)$. Therefore $\varphi^{-1}(P)$ is a prime ideal.

   Let R be a subring of S and $\varphi(r) = r$ be the inclusion map of R into S. Then $\varphi^{-1}(P) = P \cap R$ and hence $P \cap R$ is a prime ideal of R if P is a prime ideal of S.

   (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.*

   Let $\pi : S \to S/M$ be the natural projection from S to S/M and define $\psi : R \to S/M$ by $\psi = \pi \circ \varphi$. Then $\ker \psi = \{r \in R \mid \varphi(R) \in M\} = \varphi^{-1}(M)$. ψ is surjective since it is the composition of two surjective functions and

   $$R/\varphi^{-1}(M) = R/\ker \psi \cong \psi(R) = S/M$$

   M is maximal so S/M is a field, and so is $R/\varphi^{-1}(M)$. But this means $\varphi^{-1}(M)$ is maximal in R.

   To show that surjectivity is necessary, consider the inclusion map $i : \mathbb{Z} \to \mathbb{Q}$. Since $\mathbb{Q}$ is a field 0 is a maximal ideal, but the preimage of 0 is just 0, which is not maximal in $\mathbb{Z}$.

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

   If R is a commutative ring, recall that R/I is a field if and only if I is a maximal ideal. If P is a prime ideal then R/P is a finite integral domain. But every finite integral domain is a field, and therefore P is also a maximal ideal.

8. *Assume R is a commutative ring such that for every $a \in R$ there exists an integer $n > 1$ such that $a^n = a$. Prove that every prime ideal of R is maximal.*

   If P is a prime ideal of R then R/P is an integral domain. Let $a \in R$ with $a \neq 0$ and consider $a + P \in R/P$. Since $a^n = a$,

$$(a + P)(a^{n-1} + P) = (a + P)(1 + P)$$

   So that $a^{n-1} + P = 1 + P$, since R/P is an integral domain. But then, as $n \geq 2$,

$$(a + P)(a^{n-2} + P) = 1 + P$$

   So $a + P$ has an inverse in R/P, i.e., R/P is a field and hence P is a maximal ideal.

9. *Let R be a nonzero ring. Show that if e is an idempotent element of the center of R then Re and $R(1-e)$ are two-sided ideals of R and that $R \cong Re \times R(1-e)$. Show that e and $1-e$ are identities for the subrings Re and $R(1-e)$, respectively.*

   Let e be any idempotent element of the center of R, and let $r \in R$. Then

$$Re \cdot r = R \cdot er = R \cdot re = Rr \cdot e = Re$$

   so Re is a right ideal. It is obviously a left ideal, so Re is a two-sided ideal. Moreover, for any $re \in Re$,

$$e \cdot re = re \cdot e = re$$

   so that $(Re, +, \cdot)$ is a ring, though not a subring as the book says (unless it happens that $e = 1$) Note that here e was an arbitrary idempotent central element, and hence this applies to any such element.

   Consider $(1 - e)$. $1 - e$ is in the center of R since

$$r(1 - e) = r - re = r - er = (1 - e)r$$

   and is also idempotent since

$$(1 - e)^2 = 1 - 2 \cdot e + e^2 = 1 - 2 \cdot e + e = 1 - e$$

   Hence, from above, $R(1 - e)$ is a two-sided ideal of R. It also follows from above that $1 - e$ is the identity of the ring $R(1 - e)$.

   Define $\varphi : R \to Re \times R(1-e)$ by $r \mapsto (re, r(1-e))$. Then $\ker \varphi = 0$ since $(re, r(1-e)) = (0, 0)$ implies that $re = 0$ and $r = re$, and hence $r = 0$. Therefore φ is injective. To see that it is surjective, let $(re, s(1-e))$ be an arbitrary element of $Re \times R(1-e)$ and note that since e is idempotent, $e(1-e) = (1-e)e = 0$. Then $(re + s(1-e))e = re^2 + s(1-e)e = re$ and $(re + s(1-e))(1-e) = re(1-e)s(1-e)^2 = s(1-e)$. Hence φ is surjective. It is obviously a homomorphism and therefore $R \cong Re \times R(1-e)$.

   Note also that we could use the Chinese Remainder Theorem by showing that $R/Re \cong R(1-e)$ and $R/R(1-e) \cong Re$. The two ideals are obviously comaximal and their intersection is trivial, so the result follows.

10. *Let R and S be rings. Prove that every ideal of $R \times S$ is of the form $I \times J$ for I an ideal of R and J an ideal of S.*

    Let $I \times J$ be an ideal of $R \times S$ and let $(x_1, y_1), (x_2, y_2)$ be arbitrary elements of $I \times J$. Then $(x_1 + x_2, y_1 + y_2) \in I \times J$, which implies $x_1 + x_2 \in I$ and $y_1 + y_2 \in J$. Similarly, for any $(r, s) \in R \times S$, $(r, s)(x, y) = (rx, sy) \in I \times J$, which implies $rx \in I$ and $sy \in J$. Since all these points were arbitrary, I and J are ideals of R and S, respectively.

11. *Prove that if R and S are nonzero rings then $R \times S$ is never a field.*

    Pick any nonzero element $r \in R$ and $s \in S$. Then

    $$(r, 0)(0, s) = (0, 0)$$

    but neither $(r, 0)$ nor $(0, s)$ is $(0, 0)$. Hence $R \times S$ is never an integral domain, and therefore never a field.

12. *Let $n_1, n_2, \ldots, n_k$ be integers such that $(n_i, n_j) = 1$ for $i \neq j$.*

    (a) *Show that the Chinese Remainder Theorem implies that for any $a_1, \ldots, a_k \in \mathbb{Z}$ there is a solution $x \in \mathbb{Z}$ to the simultaneous congruences $x \equiv a_1 \mod n_1, \ldots, x \equiv a_k \mod n_k$.*
    If $(n_i, n_j) = 1$ for $i \neq j$ then their respective ideals $n_i\mathbb{Z}$ and $n_j\mathbb{Z}$ are comaximal, i.e., $n_i\mathbb{Z} + n_j\mathbb{Z} = \mathbb{Z}$. By the Chinese remainder theorem, letting $n = n_1 n_2 \cdots n_k$,

    $$\mathbb{Z}/n\mathbb{Z} \equiv \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

    Hence there is a surjective homomorphism φ from $\mathbb{Z}$ to $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$. Let $\overline{a_i} \in \mathbb{Z}/n_i\mathbb{Z}$. Then there exists an $x \in \mathbb{Z}$ such that $\varphi(x) = (\overline{a_1}, \ldots, \overline{a_k})$, i.e., x is congruent to a_i modulo n_i for each $1 \leq i \leq k$. This x is unique modulo n since $n\mathbb{Z}$ is the kernel of this homomorphism.

    (b) *Show that this solution x from (a) is given by $x = a_1 t_1 n_1' + \cdots + a_k t_k n_k' \mod n$ where $n_i' = n/n_i$ and t_i is the inverse of n_i' modulo n_i.*
    Since $(n_i', n_i) = 1$ there exists such a t_i. Consider n_j and $a_i t_i n_i'$ such that $i \neq j$. Then $n_j \mid a_i t_i n_i'$ since $\frac{n}{n_i n_j} = \prod_{h=1}^{k} n_h$ where $h \neq i$ and $h \neq j$. Consider $x - a_j$, where x is as above. Then

    $$x - a_j = \sum_{i=1, i \neq j}^{k} a_i t_i n_i' + a_j(t_j n_j' - 1)$$

    Hence $n_j \mid x - a_j$ since n_j divides all the summands in the sum on the left, and $t_j n_j' = 1$ modulo n_j by construction. Therefore x satisfies all the desired congruences. Modulo n, this is the unique solution.

    (c) *Solve the simultaneous system of congruences*

    $$x \equiv 1 \mod 8, \, x \equiv 2 \mod 25, \, x \equiv 3 \mod 81$$

    and

    $$y \equiv 5 \mod 8, \, y \equiv 12 \mod 25, y \equiv 47 \mod 81$$

    The smallest positive integral solutions to the above equations are $x = 4377$ and $y = 15437$.