MATH 258: Homework #2

Jesse Farmer

19 January 2005

1. *Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = 1$ or $x = -1$.*

   We know that for any $a, b \in R$ that $a^2 - b^2 = (a-b)(a+b)$, so if $x^2 = 1$ for some $x \in R$ then $x^2 - 1 = (x-1)(x+1)$. If R is an integral domain this implies that $x - 1 = 0$ or $x + 1 = 0$, i.e., $x = 1$ or $x = -1$.

2. *An element in R is called* nilpotent *if $x^m = 0$ for some $m \in \mathbb{Z}_+$.*

   (a) *Show that if $n = a^k b$ for some integers a and b then $\overline{ab}$ is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$.*

   If $n = a^k b$ then $n \mid (ab)^k$ and $\left(\overline{ab}\right)^k = (ab)^k + n\mathbb{Z} = n\mathbb{Z}$. Hence $\overline{ab}$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$.

   (b) *If $a \in \mathbb{Z}$ show that the element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if ever prime divisor of n is also a divisor of a. In particular, determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$.*

   Without loss of generality assume that $n, a > 0$ since n is nilpotent if and only if $-n$ is nilpotent. Assume every prime divisor of n is also a prime divisor of a. Define

   $$k = \max\{m \in \mathbb{Z}_+ \mid p^m \text{ divides } n \text{ for } p \text{ any prime} f\}$$

   Then $n \mid a^k$ so that $a^k \equiv 0 \pmod{n}$, i.e., $\overline{a}$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$. If $a^k \equiv 0 \pmod{n}$ then $n \mid a^k$. But divisibility is transitive, so

   $$p \mid n \Rightarrow p \mid a^k \Rightarrow p \mid a$$

   Hence every prime divisor of n is also a prime divisor of a.

   The nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ are all the elements of the form $2^i 3^j k$ for any $k \in \mathbb{Z}$, and both i, j not 0. Modulo n these are

   $$2, 2^2, 2^3, 3, 2 \cdot 3, 2^2 \cdot 3, 2^3 \cdot 3, 2 \cdot 3^2, 2^2 \cdot 3^2, 2^3 \cdot 3^2$$

   (c) *Let R be the ring of functions from a nonempty set X to a field F. Prove that R contains no nonzero nilpotent elements.*

   In general let $0 \neq x \in R$ for some ring R be nilpotent. Let m be the smallest integer such that $x^m = 0$, then $x^{m-1} \neq 0$ and $x \cdot x^{m-1} = 0$. Hence x is a zero divisor. In a field F, however, there are no zero divisors. Hence, if f is a function from some set X to a field F and $(f(x))^m = 0$ for all $x \in X$, then $f \equiv 0$.

3. *Prove that every Boolean ring is commutative.*

   Let R be a Boolean ring. Let $x, y \in R$ be arbitrary, then

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

   and hence for all $x \in R$, $x + x = 0$, or $x = -x$. Then

   $$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + yx + xy + y$$

   and hence $yx = -xy = xy$ for all $x, y \in R$, i.e., R is commutative.

4. *Let R and S be rings. Prove that the direct product $R \times S$ is a ring under component-wise addition and multiplication. Prove that $R \times S$ is commutative if and only if R and S are commutative.*

   From group theory the direct product of groups is a group under component-wise application of the operator, so that holds here. All that remains is to check if the multiplicative structure is maintained, and whether or not distributivity holds. Let $(r_i, s_i) \in R \times S$ for $i = 1, 2, 3$. The operation is associative since it is in both R and S, which can be seen from

   $$\begin{aligned} ((r_1, s_1)(r_2, s_2))\,(r_3, s_3) &= (r_1 r_2, s_1 s_2)(r_3, s_3) \\ &= (r_1 r_2 r_3, s_1 s_2 s_3) \\ &= (r_1, s_1)(r_2 r_3, s_2 s_3) \\ &= (r_1, s_1)\,((r_2, s_2)(r_3, s_3)) \end{aligned}$$

   Similarly, there is a multiplicative identity, namely $(1_R, 1_S)$. Distributivity follows since

   $$\begin{aligned} (r_1, s_1)((r_2, s_2) + (r_3, s_3)) &= (r_1, s_1)(r_2 + r_3, s_2 + s_3) \\ &= (r_1(r_2 + r_3), s_1(s_2 + s_3)) \\ &= (r_1 r_2 + r_1 r_3, s_1 s_2 + s_1 s_3) \\ &= (r_1, s_1)(r_2, s_2) + (r_1, s_1)(r_3, s_3) \end{aligned}$$

   If R and S are commutative then

   $$(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2) = (r_2 r_1, s_2 s_1) = (r_2, s_2)(r_1, r_2)$$

   Hence $R \times S$ is commutative. If $R \times S$ is commutative then

   $$(r_1 r_2, s_1 s_2) = (r_1, s_1)(r_2, s_2) = (r_2, s_2)(r_1, r_2) = (r_2 r_1, s_2 s_1)$$

   Hence R and S are commutative.

5. *Prove that for any set $X \neq \emptyset$, $(\wp(X), \triangle, \cap)$ is a Boolean ring.*

   Let $\mathcal{F}(X, \mathbb{Z}/2\mathbb{Z})$ be the set of all functions from X to $Z/2\mathbb{Z}$. This is a commutative ring under the usual addition and multiplication of functions since $Z/2\mathbb{Z}$ is a field. Define

   $$\varphi : \wp(X) \to \mathcal{F}(X, \mathbb{Z}/2\mathbb{Z})$$

   by

   $$A \mapsto \chi_A$$

where χ_A the characteristic function of A. This map is obviously injective, since if two characteristic function are equal everywhere then they are the characteristic function of the same set. For any $f \in \mathcal{F}(X, \mathbb{Z}/2\mathbb{Z})$, let $A = \{x \in X \mid f(x) = 1\}$. Then, since f can only take on the values of 0 and 1, $\varphi(A) = f$. Hence φ is surjective.

Let $A, B \in \wp(X)$, then $(\chi_A + \chi_B)(x) = 0$ if $\chi_A(x) = \chi_B(x) = 0$ or $\chi_A(x) = \chi_B(x) = 1$, since $1+1 = 0$ in $\mathbb{Z}/2\mathbb{Z}$. Therefore $\chi_A + \chi_B$ is 1 if and only if x is in A or B, but not A and B, i.e.,

$$\chi_A + \chi_B = \chi_{A \triangle B}$$

Furthermore, $(\chi_A \cdot \chi_B)(x) = 1$ if and only if $x \in A \cap B$, and hence

$$\chi_A \cdot \chi_B = \chi_{A \cap B}$$

and certainly $X \mapsto \chi_X \equiv 1$.

Therefore $(\wp(X), \triangle, \cap)$ is a commutative ring since all operations can be described in terms of operations on $\mathcal{F}(X, \mathbb{Z}/2\mathbb{Z})$, which is known to be a commutative ring. It is a Boolean ring since $\mathcal{F}(X, \mathbb{Z}/2\mathbb{Z})$ is, but, in particular, $A \cap A = A$ for all $A \in \wp(A)$.

6. *Find all the homomorphic images of $\mathbb{Z}$.*

   The only nontrivial ideals of $\mathbb{Z}$ are $n\mathbb{Z}$ for $n \in \mathbb{Z}_+$ since every such $n\mathbb{Z}$ is an ideal and the only additive subgroups of $\mathbb{Z}$ are precisely those $n\mathbb{Z}$. From the first isomorphism theorem for rings it follows then that every homomorphic image of $\mathbb{Z}$ is isomorphic to either the trivial ring, $\mathbb{Z}$, or $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{Z}_+$.

7. *Describe all the ring homomorphisms from the ring $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$. In each case describe the kernel and the image.*

   Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be a ring homomorphism. Then, since $\mathbb{Z}$ is an integral domain and $f(1,0)f(0,1) = 0$, either $f(1,0) = 0$ or $f(0,1) = 0$. Also note that $f(1,0) = 1 - f(0,1)$ since $f(1,1) = 1$. Hence if $f(1,0) = 0$ then $f(0,1) = 1$ and vice versa.

   Now, it is clear from the additive properties of homomorphisms that $f(m,0) = mf(1,0)$ for all $m \in \mathbb{Z}$ and, hence for all $m, n \in \mathbb{Z}$ that

   $$f(m,n) = mf(1,0) + n(1 - f(1,0))$$

   Since $f(1,0)$ must be either 0 or 1, this implies that either $f(m,n) = m$ or $f(m,n) = n$. Both of these are obviously homomorphisms, and hence are the only homomorphisms. Denote them as f_m and f_n, respectively. Then

   $$\ker f_m = \{(0,n) \mid n \in \mathbb{Z}\} \text{ and } \ker f_n = \{(m,0) \mid m \in \mathbb{Z}\}$$

   Each of these is isomorphic to $\mathbb{Z}$ and hence the image is isomorphic to $\mathbb{Z}$. In fact, it is $\mathbb{Z}$, since the maps are surjective.

8. *Decide which of the following are ring homomorphisms from $M_2(\mathbb{Z})$ to $\mathbb{Z}$:*

   (a) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a$

   This is not a ring homomorphism since

   $$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \mapsto a_1a_2 + b_1c_2 \neq a_1a_2$$

(b) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a + d$

This is not a ring homomorphism since the multiplicative identity for $M_2(\mathbb{Z})$ is sent to 2, not 1.

(c) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$

This is not a ring homomorphism since $\det(A + B) \neq \det(A) + \det(B)$ for all $A, B \in M_2(\mathbb{Z})$. For example, let A have zero in every entry but the first column of the first row where there is a 1, and let B be zero everywhere except in the second column and second row where there is a 1. Then the determinant of the sum is 1, but the sum of the determinants is 0.

9. *Let I and J be ideals of R.*

(a) *Prove that $I + J$ is the smallest ideal of R containing both I and J.*
$I + J$ is an ideal since for $a_1, a_2 \in I$ and $b_1, b_2 \in J$

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I + J$$

and for $r \in R$

$$r(a_1 + b_1) = ra_1 + rb_1 \in I + J$$

Since $0 \in I$ and $0 \in J$, both $I \subset I + J$ and $J \subset I + J$. So $I + J$ is an ideal containing I and J. If K is an ideal containing I and J then it contains all $i + j$ where $i \in I$ and $j \in J$ by the definition of an ideal, so that $I + J \subset K$. Hence $I + J$ is the smallest such ideal.

(b) *Prove that IJ is an ideal contained in $I \cap J$.*
IJ is clearly a subgroup since the sum of two finite sums is itself a finite sum, and the additive inverse of a finite sum is just the finite sum of the additive inverses of the summands using the distributive property. Similarly, IJ is closed under left and right multiplication in R by the left and right distributive properties, and the fact that $ra_i \in I$ and $b_i r \in J$ for any $a_i \in I$, $b_i \in J$, and $r \in R$. Let

$$y = \sum_{i=1}^{r} a_i b_i \in IJ$$

Recall that both I and J are ideals, i.e., closed under both left and right multiplication in R. Then $y \in I$ since $a_i b_i \in I$ for each $1 \leq i \leq r$, and I is closed under addition. Similarly $y \in J$ since $a_i b_i \in J$ for all $a_i \in I$, and J is closed under addition.

(c) *Given an example where $IJ \neq I \cap J$.*
Let $I = 2\mathbb{Z}$ and $J = 4\mathbb{Z}$. Then $I \cap J = 4\mathbb{Z}$, but everything in IJ is a multiple of 8, so $4 \in (I \cap J) \setminus IJ$.

(d) *Prove that is R is commutative and if $I + J = R$ then $IJ = I \cap J$.*
If $I + J = R$ then, in particular $1 \in I + J$. Let $1 = i + j$ for some $i \in I$ and $j \in J$. Let $k \in I \cap J$, then

$$k = (i + j)k = ik + jk = ik + kj \in IJ$$

since $k \in I \cap J$ and R is commutative. The opposite inclusion follows from above, and hence $IJ = I \cap J$.

10. *Let I, J, K be ideals of R.*

(a) *Prove that $I(J+K) = IJ + IK$ and $(I+J)K = IK + JK$.*
The first equality follows from left distributivity:

$$\begin{aligned} I(J+K) &= \left\{ \sum_{i=1}^{r} a_i(b_i + c_i) \mid a_i \in I, b_i \in J, c_i \in K, r \in \mathbb{Z}_+ \right\} \\ &= \left\{ \sum_{i=1}^{r} (a_i b_i + a_i c_i) \mid a_i \in I, b_i \in J, c_i \in K, r \in \mathbb{Z}_+ \right\} \\ &= \left\{ \sum_{i=1}^{r} a_i b_i + \sum_{i=1}^{r} a_i c_i \mid a_i \in I, b_i \in J, c_i \in K, r \in \mathbb{Z}_+ \right\} \\ &= IJ + IK \end{aligned}$$

Though each sum has r summands it does not actually matter, since the shorter of the two sums can be padded with zeros so that both sums have the same (finite) number of summands. The second equality follows *mutatis mutandis*, with right distributivity used instead of left distributivity.

(b) *Prove that if $J \subseteq I$ then $I \cap (J+K) = J + (I \cap K)$.*
It is sufficient to prove that $j \in J, k \in K$ and $i + k \in I$ if and only if $j \in J$ and $k \in I \cap K$ since these are precisely the conditions for $i + j$ being contained in $I \cap (J+K)$ and $J + (I \cap K)$, respectively. Let j, k be as in the former case, then since $j \in J \subset I$, and $j + k \in I$, $k \in I$. Hence $k \in I \cap K$. Likewise, let j, k be as in the latter case, then $j \in I$ as before, and hence, since $k \in I \cap K$, $i + j \in I$.