# MATH 258: Homework #1

Jesse Farmer

12 January 2005

1. *Show that $(-1)^2 = 1$.*

   It is sufficient to show that $(-1)^2 + -1 = 0$ since additive inverses are unique. Note that for any $a \in R$, $a \cdot 0 = 0$ since $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$.

   $$(-1)^2 + -1 = -1 \cdot -1 + -1 \cdot 1 = -1 \cdot (-1 + 1) = -1 \cdot 0 = 0$$

2. *Show that is $u$ is a unit in $R$ then so is $-u$.*

   Note that for any $a \in R$, $-a = -1 \cdot a = a \cdot -1$ since

   $$-1 \cdot a + a = -1 \cdot a + 1 \cdot a = (-1 + 1) \cdot a = 0$$

   The second equality follows by using right distributivity. Let $u \in R$ be a unit, then there exists $v \in R$ such that $uv = 1$. Consider $-u \cdot -v$:

   $$-u \cdot -v = (-1 \cdot u) \cdot (v \cdot -1) = -1 \cdot (u \cdot v) \cdot -1 = -1 \cdot 1 \cdot -1 = (-1)^2 = 1$$

   from the previous problem.

3. *Let $R$ be a ring with identity and let $S$ be a subring of $R$ containing the identity. Prove that if $u$ is a unit in $S$ then $u$ is a unit in $R$. Show by example that the converse is false.*

   Let $u \in S \subset R$ be a unit in $S$ Then there exists a $v \in S \subset R$ such that $uv = 1 \in S \subset R$, hence $u$ is also a unit in $R$. An obvious example of the converse being false is $\mathbb{Z}$ as seen as a subring of $\mathbb{Q}$. $\mathbb{Z}$ has no units, but in $\mathbb{Q}$ each of those is a unit.

4. *Prove that the intersection of any nonempty collection of subrings of a ring is also a ring.*

   Let $R$ be a ring and $\{R_\alpha\}$ be a collection of subrings of $R$ with $R_\alpha \neq \emptyset$ for all $\alpha$ in the (arbitrary) indexing set. We know from group theory that the arbitrary intersection of subgroups of a group is itself a subgroup, so it is only necessary to check that the product and identity are preserved.

   $$1 \in \bigcap_\alpha R_\alpha \Leftrightarrow 1 \in R_\alpha \text{ for all } \alpha$$

   which is certainly true. Furthermore, let $a, b \in \bigcap_\alpha R_\alpha$, then $a, b \in R_\alpha$ for all $\alpha$ and

   $$ab \in \bigcap_\alpha R_\alpha \Leftrightarrow ab \in R_\alpha \text{ for all } \alpha$$

   which is also true. Hence $\bigcap_\alpha R_\alpha$ is a subring of $R$.

5. *Decide which if the following are subrings of $\mathbb{Q}$:*

   We will use the definition from class, i.e., that a ring contains a multiplicative identity.

   (a) *The set of all rational numbers with odd denominators, in lowest terms.*

      The denominator of both the sum and product of a rational number is the product of the denominators. Since the product of any two odd numbers is itself odd this set is closed under both addition and multiplication. That the inverse of such a number also has an odd denominator is obvious, and hence this set is a subring of $\mathbb{Q}$.

   (b) *The set of all rational numbers with even denominators, in lowest terms.*

      As 1 does not have an even denominator, this is not a subring.

   (c) *The set of nonnegative rational numbers.*

      This set is not a subgroup of $\mathbb{Q}$ under addition since no nonzero number here has an additive inverse, and therefore is not a subring.

   (d) *The set of squares of rational numbers.*

      This is not a subring. For example, 4 is the square of a rational but $4 + 4$ is not; it is irrational.

   (e) *The set of all rational numbers with odd numerators, in lowest terms.*

      Since the fractions are in lowest terms, both the numerator and denomator cannot be even, hence the denominators must be odd. Since the product of any two odd numbers is odd, and both the product and sum of even numbers is even, it follows that, for $q_1, q_2 \notin 2\mathbb{Z}$ and $p_1, p_2 \in \mathbb{Z}$,
      $$\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_1}{q_1 q_1}$$
      has an even numerator and hence is in the set. That the product of two such numbers, the additive inverse, and the multiplicative identity are in this set is clear, and hence it is a subring.

   (f) *The set of all rational numbers with even numerators, in lowest terms.*

      As the identity 1 has an odd numerator, this is not a subring.

6. *Decide which of the following are subrings of the ring of all functions from $[0, 1]$ to $\mathbb{R}$:*

   (a) *The set of all functions $f(x)$ such that $f(q) = 0$ for all $q \in \mathbb{Q} \cap [0, 1]$.*

      The function $f(x) = 1$ does not satisfy this condition and hence it is not a subring.

   (b) *The set of all polynomial functions.*

      Denote this set at $\mathbb{R}[x]$. Clearly $1 \in \mathbb{R}[x]$. Let $p(x) = \sum_{i=0}^{n} a_i x^i$ and $q(x) = \sum_{i=0}^{m} b_i x_i$. Assume $n \leq m$ without loss of generality. Then

      $$(p + q)(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{m} (a_i + b_i) x^i \in \mathbb{R}[x]$$

and

$$(pq)(x) = \left( \sum_{i=0}^{n} a_i x^i \right) \left( \sum_{j=0}^{m} b_j x^j \right)$$

$$= \left( \sum_{j=0}^{m} \left( \sum_{i=0}^{n} a_i x^i \right) b_j x^j \right)$$

$$= \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j}$$

$$= \sum_{k=0}^{n+m} c_k x^k \in \mathbb{R}[x]$$

where $c_k = \sum_{l=0}^{n} a_l b_{n-l}$. That the additive inverse of a polynomial is itself a polynomial is obvious, and hence $\mathbb{R}[x]$ is a subring.

(c) *The set of all functions which have only a finite number of zeros, together with the zero function.*

The set of all zeros of the product of two functions is the union of the zeros of both functions. Likewise, the set of all zeros of the sum of two functions is the intersection of the zeros of both functions. If both functions have a finite number of zeros then the union and intersection of their sets of zeros is of course finite, so this set is a subring (it clearly contains the identity, which has no zeros).

(d) *The set of all functions which have an infinite number of zeros.*

This is not a subring since the sum of two functions has a zero at a point if and only if both functions have a zero there. For example, the characteristic functions of the rational and irrational numbers in $[0, 1]$ has a nonzero sum, even though both have an infinite number of zeros. Additionally, it does not contain the identity.

(e) *The set of all functions such that $\lim_{x \to 1^-} f(x) = 0$.*

The identity is not such a function, and hence this is not a subring.

(f) *The set of all rational linear combinations of functions $\sin nx$ and $\cos mx$, where $m, n \in \mathbb{N}$.*

Though this set obeys the rules for summation and contains the identity and additive inverses, it is not closed under multiplication. For example, $\sin(2x)\cos(x) = 2\sin(x) - \sin^3(x)$, which cannot be written as a rational linear combination of sine and cosine functions.

7. *Prove that the center of a ring is a subring that contains the identity. Prove that the center of a division ring is a field.*

Denote the center of $R$ by $R^\times$. Trivially $1 \in R^\times$, so consider $a, b \in R^\times$ and $r \in R$. Recall that $-a = -1 \cdot a = a \cdot -1$ for any $a \in R$, in particular, for any $a \in R^\times$. Therefore

$$r(a+-b) = ra+r(-b) = ar+(rb)\cdot-1 = ar+(br)\cdot-1 = ar+-1\cdot(br) = ar+(-b)r = (a+-b)r$$

so $R^\times$ is a subgroup of $R$. From the definition it is obvious that $ab \in R^\times$, so that $R^\times$ is a subring of $R$. If $R$ is a division ring then every nonzero element of $R$ has an inverse. Since

a field is a commutative division ring it suffices to show that $a \in R^\times$ only if $a^{-1} \in R^\times$. Let $a \in R^\times$, then

$$a^{-1}r = a^{-1}r(aa^{-1}) = a^{-1}(ra)a^{-1} = a^{-1}(ar)a^{-1} = (a^{-1}a)ra^{-1} = ra^{-1}$$

Therefore $R^\times$ is a field if $R$ is a division ring.

8. *Let $X$ be any set and define $\mathcal{F}(X,\mathbb{R})$ as the set of all functions from $X$ to $\mathbb{R}$. Prove that $\mathcal{F}(X,\mathbb{R})$ is an integral domain if and only if $X$ contains exactly one element.*

   If $X$ has only one element, $x$, then $\mathcal{F}(X,\mathbb{R}) \cong \mathbb{R}$ by the map $f \mapsto f(x)$ and is therefore an integral domain (and a field, to boot). Let $\mathcal{F}(X,\mathbb{R})$ be an integral domain. Choose an $A \in \mathcal{P}(X)$ and define $B = X \setminus A$. Denote the characteristic functions of $A$ and $B$ by $\chi_A$ and $\chi_B$, i.e.,

   $$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \in X \setminus A \end{cases}$$

   Then $\chi_A \cdot \chi_B \equiv 0$ and hence $\chi_A \equiv 0$ or $\chi_B \equiv 0$. This implies that $A = X$ or $A = \emptyset$, i.e., $\mathcal{P}(X)$ has two elements and therefore $X$ has only one element.

9. *Prove that $\mathcal{C}(X,\mathbb{R})$, the set of all continuous functions from $X$ to $\mathbb{R}$, is never an integral domain where $X = [0,1]$ or $X = \mathbb{R}$.*

   Define $g, f : X \to \mathbb{R}$ by

   $$f(x) = \begin{cases} 0 & x < 0 \\ x & x \geq 0 \end{cases} \quad \text{and} \quad g(x) = \begin{cases} x & x < 0 \\ 0 & x \geq 0 \end{cases}$$

   Then $fg = 0$, but $f \not\equiv 0$ and $g \not\equiv 0$. Hence $\mathcal{C}(X,\mathbb{R})$ is not an integral domain.