HOMEWORK #6 – MATH 435

DUE MONDAY MARCH 19TH

Chapter 4, Section 1: #35 For R as in Example 10, show that $S = \{f \in R \,|\, \text{f is differentiable on } (0,1)\}$ is a subring of R which is not an integral domain.

Solution: First we need to prove that S is a subring. It is certainly closed under addition and multiplication since sums and products of differentiable functions are differentiable. It also has the additive identity since the constant function $f(x) = 0$ is differentiable. Finally, if $f \in S$, then certainly $-f$ is differentiable also and so $-f \in S$. These are all we have to prove to demonstrate that S is a subring.

Now, we must prove that S is not an integral domain. Consider the functions defined on the domain $(0,1)$.

$$f(x) = \begin{cases} 0, & x \leq \frac{1}{2} \\ (x-\frac{1}{2})^2, & x \geq \frac{1}{2} \end{cases} \qquad g(x) = \begin{cases} (x-\frac{1}{2})^2, & x \leq \frac{1}{2} \\ 0, & x \geq \frac{1}{2} \end{cases}$$

Note that f is differentiable since the derivative (from the left) of f at $\frac{1}{2}$ is 0, and the derivative from the right is also $2(\frac{1}{2} - \frac{1}{2})^1 = 0$. Likewise for g. Thus both $f, g \in S$. But then notice that $f \cdot g = 0$ (since $(f \cdot g)(x) = f(x)g(x)$ and either $f(x) = 0$ or $g(x) = 0$ for any $x \in (0,1)$. This completes the proof.

Chapter 4, Section 2: #2 If R is an integral domain and $ab = ac$ for $0 \neq a \in R$ and some $b, c \in R$, show that $b = c$.

Solution: Note $ab = ac$ implies that $ab - ac = 0$ and so $a(b-c) = 0$. Thus $a = 0$ (which is impossible since we assumed $a \neq 0$) or $b - c = 0$ (which is the only remaining possibility). Thus $b = c$ and we are done.

Chapter 4, Section 2: #3 If R is a finite integral domain, show that R is a field.

Solution: Our first order of business is to prove that R contains 1. Choose $x \in R$ nonzero. Then $x^n = x^m$ for some integers $n < m$ (by the pigeon hold principal). Consider now x^{m-n}. For any $y \in R$, we observe that

$$(yx^{m-n})x^n = yx^m = yx^n$$

and so by cancelation, $yx^{m-n} = y$. But this holds for all y and so x^{m-n} is a multiplicative identity (note the ring is commutative). Now we need to show that multiplicative inverses exist. But if $1 = x^{m-n}$ for some $m > n+1$ (which we can always arrange again by the pigeon hole principal), then x^{m-n-1} is the multiplicative inverse of x.

Chapter 4, Section 2: #5 Let R be a ring for which $x^3 = x$ for all $x \in R$. Prove that R is commutative.

Solution: Part of this proof is due to Robin Chapman and was found on the following website: (it obviously uses ideas lots of people were talking about also with me in office hours also).

http://www.math.niu.edu/~rusin/known-math/99/commut_ring

First we notice that $x^3 = x$ for all $x \in R$, so that means $(2x)^3 = 2x$ and thus $8x = 8x^3 = 2x$ and so $6x = 0$. Thus $3x = -3x$ for all $x \in R$.

We also know

$$0 = (x+y) - x - y = (x+y)^3 - x^3 - y^3 = x^2y + xyx + yx^2 + xy^2 + yxy + y^2x$$

and plugging in $y = x^2$ yields

$$0 = 3x^4 + 3x^5$$

and so using that $x^3 = x$, we have

$$0 = 3x(x^3) + 3x^2(x^3) = 3x^2 + 3x^3 = 3x^2 + 3x$$

This holds for any x. Thus

$$3x^2 = -3x = 3x$$

for any x. Plugging in now $x = x + y$ we get:

$$3x + 3y = 3(x+y) = 3(x+y)^2 = 3x^2 + 3xy + 3yx + 3y^2 = 3x + 3xy + 3yx + 3y$$

and so

$$0 = 3xy + 3yx$$

Thus $3xy = 3yx$. This is a good start!

Now, we notice the following (as pointed out in office hours):

$$0 = 0 + 0 = \left((x+y)^3 - x^3 - y^3\right) + \left((x-y)^3 - x^3 + y^3\right) = 2xy^2 + 2yxy + 2y^2x$$

Multiplying through on the left and right by y we get:

$$0 = 0+0 = y(2xy^2+2yxy+2y^2x)-(2xy^2+2yxy+2y^2x)y = 2yxy^2+2y^2xy+2y^3x-2xy^3-2yxy^2-2y^2xy$$

which is just

$$0 = 2y^3x - 2xy^3 = 2yx - 2xy$$

and so $2yx = 2xy$. Subtracting this from $3xy = 3yx$ gives us $xy = yx$ which completes the proof.

Chapter 4, Section 2: #8 If F is a finite field, show that

(a) There exists a prime p such that $pa = 0$ for all $a \in F$.
(b) If F has q elements, then $q = p^n$ for some integer n.

Solution: First we prove (a). We let $n = |F|$. By Lagrange's theorem, we know $na = 0$ for all $a \in F$. Let p be the smallest positive integer such that $p(1) = 0$ where 1 is the multiplicative identity of F. We will prove that p is prime so suppose that $p = nm$ is composite with $n, m > 1$. Then

$$0 = nm(1) = (n1)(m1).$$

Since every field is an integral domain, we thus know $n1 = 0$ or $m1 = 0$. But either leads to a contradiction since p is the smallest integer such that $p1 = 0$. Thus p is prime. But now if $p1 = 0$, then we notice that $px = (p1)(x) = 0x$ for any $x \in R$ and so $px = 0$ for all $x \in R$ which completes the proof.

Now we prove (b). Suppose that $|F| = q$. Now, we know that the p from part (a) divides q by Lagrange's theorem. On the other hand, if any other prime $p' \neq p$ divides q, then by Cauchy's theorem for the additive group of F, F contains an element y of order p'. Then $p'y = 0$. But we also know that $px = 0$ and so p divides the order of x (which is p' by assumption). But this is clearly impossible since p and p' are distinct primes.