Moshe Mason Rubin

MATH 330 Homework #2

9 September 2016

2.8 $(fg)^{(n)}(x) = \displaystyle\sum_{k=1}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x)$.

Notice $\binom{n}{k} + \binom{n}{k-1} := \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n+1-k)} = n! \left[\frac{n+1-k}{k!(n+1-k)!} + \frac{k}{k!(n+1-k)!}\right] = \frac{n!(n+1)}{k!(n-k+1)!} =: \binom{n+1}{k}$. So

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \tag{1}$$

Base Case $\mathbf{n = 1}$ $\rightarrow$ $fg^{(1)} = \displaystyle\sum_{k=0}^{1} \binom{1}{k} f^{(k)}(x)\, g^{(n-k)}(x) = \binom{1}{0} f' g(x) + \binom{1}{1} f g'(x) = f'g + fg'$ which is true by product rule. ✓

Inductive step: Assume $\mathbf{(fg)^{(n)}(x) = \sum_{k=1}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x)}$ and show $\mathbf{(fg)^{(n+1)}(x) = \sum_{k=1}^{n+1} \binom{n+1}{k} f^{(k)}(x) g^{(n+1-k)}(x)}$.

$$\begin{aligned}
(fg)^{(n+1)}(x) &= \left[(fg)^{(n)}(x)\right]' \\
&= \left[\sum_{k=1}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x)\right]' \qquad \textit{by inductive hypothesis} \\
&= \Bigg[\binom{n}{0} f g^{(n)} + \binom{n}{1} f' g^{(n-1)} + \binom{n}{2} f'' g^{(n-2)} + \cdots + \binom{n}{n-2} f^{(n-2)} g'' + \binom{n}{n-1} f^{(n-1)} g' \\
&\qquad + \binom{n}{n} f^{(n)} g\Bigg]' \\
&= \binom{n}{0} f' g^{(n)} + \binom{n}{0} f g^{(n+1)} + \binom{n}{1} f'' g^{(n-1)} + \binom{n}{1} f' g^{(n)} + \binom{n}{2} f''' g^{(n-2)} \\
&\quad + \binom{n}{2} f'' g^{(n-1)} + \cdots + \binom{n}{n-2} f^{(n-1)} g'' + \binom{n}{n-2} f^{(n-2)} g''' + \binom{n}{n-1} f^{(n)} g' \\
&\quad + \binom{n}{n-1} f^{(n-1)} g'' + \binom{n}{n} f^{(n+1)} g + \binom{n}{n} f^{(n)} g' \qquad \textit{by base case} \\
&= \binom{n}{0} f g^{(n+1)} + \left(\binom{n}{0} + \binom{n}{1}\right) f' g^{(n)} + \left(\binom{n}{1} + \binom{n}{2}\right) f'' g^{(n-1)} + \cdots \\
&\quad + \left(\binom{n}{n-2} + \binom{n}{n-1}\right) f^{(n-1)} g'' + \left(\binom{n}{n-1} + \binom{n}{n}\right) f^{(n)} g' + \binom{n}{n} f^{(n+1)} g \\
&= \binom{n}{0} f g^{(n+1)} + \binom{n+1}{1} f' g^{(n)} + \binom{n+1}{2} f'' g^{(n-1)} + \cdots \\
&\quad + \binom{n+1}{n-1} f^{(n-1)} g'' + \binom{n+1}{n} f^{(n)} g' + \binom{n}{n} f^{(n+1)} g \qquad \textit{by equation (1)} \\
&= \binom{n+1}{0} f g^{(n+1)} + \binom{n+1}{1} f' g^{(n)} + \binom{n+1}{2} f'' g^{(n-1)} + \cdots + \binom{n+1}{n-1} f^{(n-1)} g'' \\
&\quad + \binom{n+1}{n} f^{(n)} g' + \binom{n+1}{n+1} f^{(n+1)} g, \quad \text{as } \tbinom{n}{0} = \tbinom{n+1}{0} = \tbinom{n}{n} = \tbinom{n+1}{n+1} = 1 \\
&= \sum_{k=1}^{n+1} \binom{n+1}{k} f^{(k)}(x) g^{(n+1-k)}(x)
\end{aligned}$$

So for all $n \in \mathbb{N}$, $(fg)^{(n)}(x) = \displaystyle\sum_{k=1}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x)$. $\square$

2.27 Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $a | bc$, then $a | c$.

By Theorem 2.4, $\gcd(a, b) = 1 \implies$ there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b) = 1$.

$a|bc \implies$ there exists $k \in \mathbb{Z}$ such that $ak = bc$ by definition. So

$$\begin{aligned} ax + by = 1 &\implies acx + bcy = c \\ &\implies acx + aky = c \quad \text{as } ak = bc \\ &\implies a(cx + ky) = c \end{aligned}$$

Because $(cx + ky) \in \mathbb{Z}$, so $a|c$ by definition.

Lemma to 2.31 Let $x \in \mathbb{Z}$ such that $2|x^2$, then $2|x$.

Consider for a contradiction that $2|x^2$ but $2 \nmid x$. Then x must be of the form $x = 2c+1$ for some $c \in \mathbb{Z}$ by the Remainder Theorem and assumption that $2 \nmid x$. Then $x^2 = c^2 + 2c + 1 = 2(c^2 + c) + 1 = 2c' + 1$. But $2 \nmid (2c' + 1)$, which is a contradiction to the assumption that $2|x^2$. So $2|x^2 \implies 2|x$.

2.31 Show $\sqrt{2} \notin \mathbb{Q}$.

Assume for a contradiction that $\sqrt{2} = \frac{p}{q}$, a fraction is lowest terms such that p and q share no divisors. Then $2 = \frac{p^2}{q^2}$.

$$\begin{aligned} 2 = \frac{p^2}{q^2} &\implies 2q^2 = p^2 \\ &\implies 2|p^2 \quad \text{by definition of divides} \\ &\implies 2|p \quad \text{by lemma to 2.31} \\ &\implies \text{There exists } k \in \mathbb{Z} \text{ such that } 2k = p \quad \text{by definition of divides} \end{aligned}$$

So,

$$\begin{aligned} 2q^2 = p^2 &\implies 2q^2 = (2k)^2 \quad \text{as } p = 2k \\ &\implies 2q^2 = 4k^2 \\ &\implies q^2 = 2k^2 \\ &\implies 2|q^2 \quad \text{by definition of divides} \\ &\implies 2|q \quad \text{by lemma to 2.31} \end{aligned}$$

But $2|p$ and $2|q$ is a contradiction as p and q were assumed to be co-prime. So our assumption that $\sqrt{2}$ can be written as a fraction is incorrect and $\sqrt{2} \notin \mathbb{Q}$. $\square$

3.1 Find all $x \in \mathbb{Z}$ satisfying each of the following equations.

(a) $3x \equiv 2 \pmod{7}$

Notice $3 \cdot 5 \equiv 15 \equiv 1 \pmod{7}$. So $3x \equiv 2 \pmod{7} \implies 5 \cdot 3x \equiv 5 \cdot 2 \pmod{7} \implies 15x \equiv 10 \pmod{7} \implies \boxed{x \equiv 3 \pmod{7}}$

(b) $5x + 1 \equiv 13 \pmod{23}$

Notice that $\gcd(23, 5) = 1$:
$$\begin{aligned} 23 &= 5q + r \quad \rightarrow \quad 23 = 5(4) + 3 \\ 5 &= 3q + r \quad \rightarrow \quad 5 = 3(1) + 2 \\ 3 &= 2q + r \quad \rightarrow \quad 3 = 2(1) + \mathbf{1} \\ 2 &= 1q + r \quad \rightarrow \quad 2 = 1(2) + 0 \end{aligned}$$

Furthermore, $3 - 2 = 1 \implies 3 - (5 - 3) = 1 \implies 2(3) - 5(1) = 1 \implies 2(23 - 5 \cdot 4) - 5 = 1 \implies 2 \cdot 23 - 9 \cdot 5 = 1 \implies 23|(1 + 9 \cdot 5) \implies -9 \cdot 5 \equiv 1 \pmod{23}$.

So $5x + 1 \equiv 13 \pmod{23} \implies 5x \equiv 12 \pmod{23} \implies -9 \cdot 5x \equiv -9 \cdot 12 \pmod{23} \implies -45x \equiv -108 \pmod{23} \implies \boxed{x \equiv 7 \pmod{23}}$

(c) $5x+1 \equiv 13 \pmod{26}$

Notice $\gcd(5,26) = 1$ and $26 - 5(5) = 1 = \gcd(5,26)$. So $5x+1 \equiv 13 \pmod{26} \implies 5x \equiv 12 \pmod{26} \implies -5(5) \equiv -5(12) \pmod{26} \implies \boxed{x \equiv 18 \pmod{26}}$

(d) $9x \equiv 3 \pmod 5$

Notice $\gcd(9,5) = 1$ and $9(4) + 5(-7) = 1 = \gcd(9,5)$. So $9x \equiv 3 \pmod 5 \implies 4 \cdot 9x = 4 \cdot 3 \pmod 5 \implies \boxed{x \equiv 12 \equiv 2 \pmod 5}$

(e) $5x \equiv 1 \pmod 6$

Notice $\gcd(5,6) = 1$ and $6 - 5 = 1 = \gcd(5,6)$. So $5x \equiv 1 \pmod 6 \implies -5x \equiv -1 \pmod 6 \implies \boxed{x \equiv 5 \pmod 6}$

(f) $3x \equiv 1 \pmod 6$

By Proposition 3.1.6, $\gcd(3,6) \neq 1 \implies$ there exists no $b \in \mathbb{Z}_n$ such that $3b = 1 \pmod 6$. So this equation has no solutions.

3.2 Which of the following multiplication tables defined on the set $G = \{a,b,c,d\}$ form a group?

(a) is not a group. a is the element such that $a \circ x = x$ for all $x \in G$, however, $x \circ a \neq x$,so (a) is not a group.

(b) is a group.

(c) is a group.

(d) is not a group because it is not associative. For example, $(b \circ c) \circ d$ should equal $b \circ (c \circ d)$, but $(b \circ c) \circ d = d$ and $b \circ (c \circ d) = a$

3.3 Write out Cayley tables for groups formed by the symmetries of a rectangle and for $(\mathbb{Z}_4, +)$.

1. Rotations of a rectangle:

$\circ$	id	ρ_{180°	μ_y	μ_x
id	id	ρ_{180°	μ_y	μ_x
ρ_{180°	ρ_{180°	id	μ_x	μ_y
μ_y	μ_y	μ_x	id	ρ_{180°
μ_x	μ_x	μ_y	ρ_{180°	id

2. $(\mathbb{Z}_4, +)$:

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

3.6 Give a multiplication table for the group $U(12)$.

$U(n) = \{x \in \mathbb{Z}_n | \gcd(n,x) = 1\} \implies U(12) = \{1,5,7,11\}$.

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

3.7 Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

An *abelian group* is a group G such that $a * b = b * a$ for all $a, b \in G$.

Associative For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

$$\begin{aligned}
(a * b) * c &= (a * b) + c + (a * b)c \quad \text{by definition of } a * b \\
&= (a + b + ab) + c + (a + b + ab)c \quad \text{by definition of } a * b \\
&= a + b + c + ab + ac + bc + abc \\
&= a + (b + c + bc) + a(b + c + bc) \\
&= a + (b * c) + a(b * c) \quad \text{by definition of } a * b \\
&= a * (b * c) \quad \text{by definition of } a * b
\end{aligned}$$

Identity element There exists an element $e \in G$ such that for any $a \in G$, $e * a = a * e = a$.

For any a, let $b = 0$. Then $a * b = a + 0 + a(0) = a = 0 + a + 0(a) = b * a$. So $b = 0$ is the identity element such that $a * 0 = 0 * a$ for all $a \in G$.

Inverse element For each element $a \in G$ there exists an $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

We know from above that $e = 0$. So given $a \in G$,

$$\begin{aligned}
a + b + ab &= 0 \\
&\implies b(1 + a) + a = 0 \\
&\implies b = \frac{-a}{1 + a}
\end{aligned}$$

which is defined for all $x \in S$. So $b = \frac{-a}{1+a}$ is the unique inverse element a^{-1} to each a such that $a * a^{-1} = a^{-1} * a = e$.

Commutative For all $a, b \in G$, $a * b = b * a$.

$$\begin{aligned}
a * b &= a + b + ab \\
&= b + a + ab \quad \text{by commutative property of addition} \\
&= b + a + ba \quad \text{by commutative property of multiplication} \\
&= b * a \quad \text{by definition}
\end{aligned}$$

So $(S, *)$ is an abelian group. $\square$

3.10 Prove that the set of matrices of the form $\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}$ is a group under matrix multiplication. Matrix multiplication in the Heisenberg group is defined by

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x + x' & y + y' + xz' \\ 0 & 1 & z + z' \\ 0 & 0 & 1 \end{bmatrix}$$

Associative For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

$$
\begin{aligned}
(a \cdot b) \cdot c &= \begin{bmatrix} 1 & a_x b_y & a_y b_y + a_x b_z \\ 0 & 1 & a_z + b_z \\ 0 & 0 & 1 \end{bmatrix} \cdot c \quad \text{by definition} \\
&= \begin{bmatrix} 1 & a_x + b_x + c_x & a_y + b_y + c_y + a_x b_z + a_x c_z + b_x c_z \\ 0 & 1 & a_z + b_z + c_z \\ 0 & 1 & 1 \end{bmatrix} \quad \text{by definition} \\
&= \begin{bmatrix} 1 & a_x + (b_x + c_x) & a_y + (b_y + c_y + b_x c_z) + a_x (b_z + c_z) \\ 0 & 1 & a_z + (b_z + c_z) \\ 0 & 0 & 1 \end{bmatrix} \\
&= a \cdot \begin{bmatrix} 1 & b_x + c_x & b_y + c_y + b_x c_z \\ 0 & 1 & b_z + c_z \\ 0 & 0 & 1 \end{bmatrix} \quad \text{by definition} \\
&= a \cdot (b \cdot c) \quad \text{by definition}
\end{aligned}
$$

Identity element There exists an element $e \in G$ such that for any $a \in G$, $e \cdot a = a \cdot e = a$.

Let $e = I_3 = \left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right]$. Then

$$
\begin{aligned}
\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} &= \begin{bmatrix} 1 & x+0 & y+0+x(0) \\ 0 & 1 & z+0 \\ 0 & 1 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0+x & 0+y+0(z) \\ 0 & 1 & 0+z \\ 0 & 1 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}
\end{aligned}
$$

So $e = I_3$ is the identity element such that $e \cdot a = a = a \cdot e$ for all $a \in G$.

Inverse element For each element $a \in G$ there exists an $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

For each $a = \left[\begin{smallmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{smallmatrix}\right] \in G$, it's inverse a^{-1} is given by the inverse matrix of a, $a^{-1} = \left[\begin{smallmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{smallmatrix}\right]$ (by linear algebra), as

$$
\begin{aligned}
a \cdot a^{-1} &= \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -x & xz - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & x + (-x) & y + (xz - y) + x(-z) \\ 0 & 1 & z + (-z) \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3 \\
&= \begin{bmatrix} 1 & (-x) + x & (xz - y) + y + (-x)z \\ 0 & 1 & (-z) + z \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & -x & xz - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \\
&= a^{-1} \cdot a
\end{aligned}
$$

So $a^{-1} = \left[\begin{smallmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{smallmatrix}\right]$ is the unique inverse element to each a such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

So the set of matrices of the form $\left[\begin{smallmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{smallmatrix}\right]$ is a group under matrix multiplication. $\square$