NON-COMMUTATIVE RINGS

ALEX THOLEN

1. What Are Non-Commutative Rings

First, let's see what rings are.

Definition 1.1. Rings are sets of numbers where

(1) Addition is associative: $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$.

(2) Addition is commutative: $a + b = b + a$ for all $a, b \in R$.

(3) There is an additive identity $0 \in R$ such that $a + 0 = 0 + a = a$ for all $a \in R$.

(4) Each element has an additive inverse: for every $a \in R$, there is an element $-a \in R$ so that $a + (-a) = 0$.

(5) Multiplication is associative: $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in R$.

(6)There is a multiplicative identity $1_{Left} \in R$ and $1_{Right} \in R$ so that $a \times 1_{Right} = 1_{Left} \times a = a$ for all $a \in R$.

(7) Distributive law: $a \times (b + c) = (a \times b) + (a \times c)$.

Remark 1.2. Note that multiplication need not be commutative. Also, note that we do not necessarily have multiplicative inverses.

Definition 1.3. Non-Commutative rings are rings where multiplication is not commutative: i.e. $a \times b \neq b \times a$ for some $a, b \in R$.

Remark 1.4. We normally write $a \times b$ as $a \cdot b$, or even as ab.

Example. The matrix ring of $n \times n$ matrices over the real numbers, where $n > 1$.

Example. Hamilton's quaternions

2. Some Basic Uses

Let's begin with the basics.

Proposition 2.1. *(1)* $1_{Left} = 1_{Right}$.

(2) The additive and multiplicative identities 0 and 1 are unique

(3) Additive inverses are unique

(4)$(-1) \times (-1) = 1$

(5) For any $a \in R$, $a \times 0 = 0 \times a = 0$.

(6)For any $a \in R$, $(-1) \times a = -a$.

Proof. (1) We look at $1_{Left} \times 1_{Right}$. Since 1_{Left} is a left identity, we get $1_{Left} \times 1_{Right} = 1_{Right}$. Also, since 1_{Right} is a right identity, we get $1_{Left} \times 1_{Right} = 1_{Left}$. So, $1_{Right} = 1_{Left}$. (2) Assume that there are two 0's. Say 0 and $0'$. Then, add them up. $0 + 0' = 0$ and $0' + 0 = 0'$. That means, $0 = 0'$.

Date: June 30, 2017.

Assume that there are two $1's$. Say 1 and $1'$. Then, multiply them. $1 \times (1') = 1$ and $(1) \times 1' = 1'$. That means, $1 = 1'$.

(3) Assume there are two additive inverses of a, $-a$ and $-a'$. We have $-a + a - a' = (-a + a) - a' = -a'$ and $-a + a - a' = -a + (a - a') = -a$. So, $-a = -a'$.

(4) $(-1)\times(1+-1) = (1)\times(0) = 0$ and $(-1)\times(1+-1) = -1\times1+-1\times-1 = -1+-1\times-1 = 0$, so $-1 \times 1 + -1 \times -1 = -1 + -1 \times -1 = 0$. Solving, we get $-1 \times -1 = 0 - -1 = 1$.

(5) $a \times (x + 0) = a \times x = a \times x + a \times 0$. So, $a \times 0 = 0$.

(6) $a\times(1-1) = a\times1+a\times-1 = 0$. So, $a+-1*a = 0$, or $a = -(-1*a)$, or $-a = -1*a$. ■

Definition 2.2. Let R be a ring. A subset of I is termed: A **left ideal** of R if I is a subgroup of R under + and if $rx \in I$ for any $r \in R$ and $x \in I$ (note that the name comes from the element being on the left)

Definition 2.3. A **right ideal** of R if I is a subgroup of R under + and if $rx \in I$ for any $r \in R$ and $x \in I$

Definition 2.4. A **two-sided ideal** of R if it is both a left and a right ideal.

3. Quaternions

Now that we have figured out the basic things on non-commutative rings, let's look at one of the examp;les. Let's look at Hamilton's Quaternions. Or rather, we will look at it's polynomial ring. Let's first define what the Quaternions are.

Definition 3.1. The Quaternions, denoted by $\mathbb{H}$, are $\mathbb{R}^4$ where we denote (a, b, c, d) as $a + bi + cj + dk$, and

$$(1)\quad ij = k$$
$$(2)\quad ji = -k$$
$$(3)\quad jk = i$$
$$(4)\quad kj = i$$
$$(5)\quad ki = j$$
$$(6)\quad ik = -j$$
$$(7)\quad ijk = i^2 = j^2 = k^2 = -1$$

Let's begin by looking at multiplication.

Definition 3.2. Multiplication by a constant is just multiplication in the reals, applied to the $1, i, j, k$ cooefficients.

Question 3.3. *How do you express $m\times n$, where $m = a+bi+cj+dk$ and $n = w+xi+yj+zk$?*

Let's write it out. We have $(a + bi + cj + dk) \times (w + xi + yj + zk)$. If we expand, we get $(aw + bixi + cjyj + dkzk) + (axi + biyj + cjzk + dkw)+ (ayj + bizk + cjw + dkxi) + (azk + biw + cjxi + dkyj)$. Since we can move constants to the sides, we get $(aw + bxi^2 + cyj^2 + dzk^2) + (axi + byij + czjk + dwk)+ (ayj + bzik + cwj + dxki) + (azk + bwi + cxji + dykj)$ We now how to multiply each of $1, i, j, k$, so we get

$$m\times n = (aw-bx-cy-dz)+(ax+bw+cz-dy)i+(ay-bz+cw+dx)j+(az+by-cx+zw)k$$

Next up is figuring out how you inverse numbers. We have $\frac{1}{a+bi+cj+dk} = w + xi + yj + zk$. So, we expand, to get $aw - bx - cy - dz = 1$ $ax + bw + cz - dy = 0$ $ay - bz + cw + dx = 0$ $az + by - cx + dw = 0$ Eventually, you get $w + xi + yj + zk = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$

Let's define the absolute value.

Definition 3.4. We will define the absolute of $x = a+bi+cj+dk$ to be $|x| = \sqrt{a^2 + b^2 + c^2 + d^2}$

Let's see what properties it has.

Question 3.5. *Is* $|ab| = |a||b|$*?*

Let's see if this is true. We want $|(a + bi + cj + dk)(e + fi + gj + hk)| = |a + bi + cj + dk||e + fi + gj + hk|$. Let's expand each thing. We have

$$\sqrt{(ae - bf - cg - dh)^2 + (af + bg + ch - de)^2 + (ag - bh + ce + df)^2 + (ah + bg - cf + de)^2}$$
$$= \sqrt{(a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2)}.$$

When you expand the left side though, there are negatives that don't get accounted for. That means that absolute values does not multiply :(Now, let's look at the quaternions polynomial ring.

Definition 3.6. We will define the polynomial ring $\mathbb{H}[x]$ to be

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0,$$

where $a_1, a_2, ..., a_n \in \mathbb{H}$.

So, let's look at some simple polynomials and their roots. Let's begin with just the single degree.

So, we have $f(x) = ax + b$. Obviously, the roots should only be $-\frac{b}{a}$. Let's prove this. We want to show that if $ar + b = 0$, then $r = -\frac{b}{a}$. We first subtract b, giving $ar = -b$. Then, we left multiply by $\frac{1}{a}$, giving $r = -\frac{1}{a}b$. Just as we expected.

Next, let's look at some quadratics.

Let's begin with the most simple one. We have x^2. We want to show that there are no 0 roots, other than 0. So, let's see if everything has an inverse. We can see that the only reason something wouldn't have a square root is if $a^2 + b^2 + c^2 + d^2 = 0$. Since a, b, c, d are reals, the only way that is possible is if $a = b = c = d = 0$. So, only 0 has no inverse. That means that if $x^2 = 0$, we can multiply by $\frac{1}{x}$ twice, if $x \neq 0$, to get $1 = 0$. That is wrong, so the only root of 0 is 0.

Now, let's look at a slightly more complex one. We will look at $x^2 + 1 = 0$. That means that $x^2 = -1$. Obviously, i, j, k work. So, does -1 have more than 3 square roots? Yes it does actually. If we look at anything of the form $bi + cj + dk$ where $b^2 + c^2 + d^2 = 1$, then we get $x^2 = -1$. However, is that all of them? Can we prove that those are all of them? We want

$aa - bb - cc - dd = -1$
$ab + ba + cd - dc = 0$
$ac - bd + ca + db = 0$
$ad + bc - cb + da = 0$

Solving, we get $b^2 + c^2 + d^2 = 1$ and $a = 0$. Using this, we have shown that if we have $x^2 + n = 0$, then the solutions are $b^2 + c^2 + d^2 = -n$.

If we look at $x^2 - 1 = 0$, then we get the same equations except for that $a^2 - b^2 - c^2 - d^2 = 1$. Then, the only solution is $a^2 = 1$, or $a = \pm 1$. So, the only two roots to $x^2 - 1$ are $1, -1$. Using this, we have shown that if we have $x^2 - n = 0$, then the solutions are $\pm\sqrt{n}$.