DIVISION RINGS AND WEDDERBURN'S THEOREM

ANUJ THAKUR

1. Summary

This paper focuses on certain rings known as division rings and a theorem known as Wedderburn's Little Theorem. First we define a division ring,

Definition 1.1. A *division ring* R is a ring where all non-zero elements have multiplicative inverses, i.e. for any non-zero element $a \in R$, there exists $b \in R$ such that $ab = ba = 1$. Division rings are sometimes referred to as *skew rings*.

In short, division rings are rings in which the operation of division is well-defined. Division rings have applications to Linear Algebra as well which we will go over later in the paper.

2. Wedderburn's Little Theorem

Theorem 2.1 (Wedderburn's Little Theorem)**.** *Every finite division ring is a field.*

While there are multiple approaches to proving Wedderburn's Little Theorem, we will be focusing on a ring-theoretic version. This proof is due to [**?**]. To begin, we prove a series of lemmas, definitions and propositions.

Definition 2.2. The *characteristic* of a field is the number of times any element must be applied in a sum to obtain the additive identity. If there exists some element that cannot be added to itself a finite number of times to achieve the additive identity, the characteristic is said to be 0.

Example. If the characteristic of a field F is 3, for all $a \in F$, $a + a + a = 0$.

Proposition 2.3. *If a ring does not have any nontrivial zero divisors, the characteristic is 0 or prime.*

Lemma 2.4. *Suppose that F is a finite field with non-zero $a, b \in F$. Then there exist some $c, d \in F$ such that $ac^2 + bd^2 + 1 = 0$.*

Proof. Since the field is finite, the characteristic of F must be nonzero.

If the characteristic of the field F is 2, then the order of the field can be expressed as 2^n for some n. Then, all elements in the field satisfy $x^{2^n} = x$ and hence every element is a square. Thus $\alpha = a^2$ for some $a \in F$. Letting $d = 0$ yields

$$ac^2 + bd^2 + 1 = (\alpha)(\alpha^{-1}) + 0 + 1 = 1 + 1 = 0$$

because the characteristic is 2.

Date: July 13, 2020.

Now we start by letting our characteristic be p where p is odd. Then for some n, the field F has p^n elements($n \in N$). We then look to count the number of elements in $1 + ax^2$ which is $1 + \frac{(p^n-1)}{2}$. We want to do this again for $-by^2$. Similarly we get that this second set has the exact same number of elements. By the pigeonhole principle, there exists at least one element that is in both of the sets(let it be g). This means that we have $g = 1 + ax^2$ and $g = -by^2$. Equating and re-arranging gives us $ax^2 + by^2 + 1 = 0$ as desired.

□

Lemma 2.5. *For every $a \in R$, define $g_a : R \to R$ as $g_a(x) = xa - ax$. Then, the function g_a satisfies*

$$g_a^m(x) = \sum_{j=0}^{m} (-1)^j \binom{m}{j} a^j x a^{m-j}.$$

This lemma requires quite a bit of combinatorial manipulation as well as induction to prove. The proof can be found in [**?**].

Definition 2.6. The *center* of a ring is a non-zero ring where every non-zero element has a multiplicative inverse.

Definition 2.7. The *prime subfield* of F is the intersection of all the subfields of F.

Proposition 2.8. *Suppose D is a division ring with a characteristic of $p > 0$ and center Z and prime subfield $P = 0, 1, \ldots, p-1$. Then if we take $a \in D$ but not in Z then there exists some $x \in D$ such that*

(1) $xax^{-1} \in P(a)$
(2) $xax^{-1} \neq a$
(3) $xax^{-1} = a^i$ *for some* $i \geq 2$

Note that $P(a)$ is the field when we add a as an element to the field P.

The proof of this proposition is similar to the proof of Lemma 3.3 and uses the map defined in Lemma 3.4. We will omit it in this paper for conciseness.

Now we are ready to prove the original statement.

Proof of Theorem 3.2. Let D be a finite division ring. To show that it is a field we have to show that it is commutative. We show this by using induction on the number of elements in D. Suppose that Z is the center of D and that Wedderburn's theorem holds for all division rings of order less than $|D|$. In our proof we make a series of claims.

Claim 1. If $a \in D$ and $a \in Z$ where a is an element with the smallest order relative to Z. Then this order must be prime.

The proof of this is a proof by contradiction that uses arguments of minimality. We shall refer to this order as r for the remainder of the proof.

□

Assume now for the sake of contradiction that D is not a field. From Claim 1 we know that we can find an a such that its order is minimal relative to Z. Suppose now that we have a with minimal order of r relative to Z and that a is not an element of Z. Applying the third part of Proposition 3.9 tells us that there exists $x \in D$ such that $xax^{-1} = a^i$ and $xa = ax$. Now we look at x^2ax^{-2}. This is equal to $x(xax^{-1})x^{-1} = x(a^i)x^{-1} = (xax^{-1})^i = a^{i^2}$. We can easily see inductively that $x^{r-1}ax^{-(r-1)} = a^{i^{r-1}}$.

We see r does not divide i and that r is prime so $i^{r-1} \equiv 1(\text{mod p})$ by Fermat's Little Theorem. Thus there exists an integer c such that $i^{r-1} = 1 + cr$. Now let $\lambda = a^{cr}$. Then we have that $a^{i^{r-1}} = a^{1+cr} = aa^{cr} = a\lambda = \lambda a$.

Claim 2. $\lambda \neq 1$.

Proof. Assume for contradiction that $\lambda = 1$. Then $x^{r-1}a = \lambda ax^{r-1}$ is $x^{r-1}a = ax^{r-1}$. Then we have that $x^{r-1} \in Z$ but this contradicts our minimality from Claim 1 because r is the smallest integer with $a^r \in Z$. Hence we must have $\lambda \neq 1$.

□

Claim 3 For some $y \in D$ and $y^r = 1$ then $y = \lambda^i$.

This proof follows based on contradictions from Claims 1 and 2.

□

It is known that every finite multiplicative group of a field is cyclic. In particular, we are concerned with the center of the field, Z which is also cyclic. We now suppose l is a generator of Z. We know that $a^r \in Z$ and that $b^r \in Z$. From this we have that $a^r = l^n$ and $b^r = l^m$. Using Claim 3 implies that $a/l^r = \lambda^i \rightarrow a = l^r\lambda^i \in Z$.

However, this is a contradiction though, because throughout this proof we have assumed that a is not in Z. However, our proof of minimality was not flawed so we must have that r does not divide n or m. Now let $a_1 = a^n$ and $b_1 = b^m$. We have that $ba = \lambda ab$ which is equivalent to $bab^{-1} = \lambda a$. We have that $\lambda \in Z$ so $ba_1b^{-1} = \lambda^n a_1$. Because r doesn't divide n or m and is prime it follows that r doesn't divide nm either. This means that $\lambda^{-mn} \neq 1$, leading us to our last claim.

Claim 4. We have $(a_1^{-1}b_1)^r = (\lambda^{-mn})^{r(r-1)/2}$.

This claim can be proven simply with induction on r.

□

To prove Wedderburn's theorem now we apply the results of the Lemmas and Claims we have made throughout this paper.

If r is an odd prime, $v^r = 1$ implies that $v^{r(r-1)/2} = 1$. By Claim 4 this means that $(a_1^{-1}b_1)^r = 1$. But because $a_1^{-1}b_1$ satisfies the $y^r = 1$ condition from Claim 3 we have that $a_1^{-1}b_1 = \lambda^i$ for some i. However this implies that $b_1a_1 = va_1b_1$ but this means that $v = 1$ which contradicts $v \neq 1$ which in turn shows that D is a field because we assumed it not to be at the beginning of our proof. Thus the proof is complete for odd primes.

■

3. Conclusion

Division rings, as mentioned before have many applications one of them being to linear algebra. Typically in linear algebra, we imagine vector spaces over a field but with the introduction of division rings we can imagine modules over a division ring and many of the critical proofs hold.

Oftentimes in the study of ring-theory non-commutative rings are overlooked. There has been a lot of excitement the past few decades regarding the applications of these non-commutative rings, some of these fields include lie algebra and computer vision.