Chapter 7. Selected Topics

Section 7.2. Wedderburn's Theorem on Finite Division Rings

Note. Joseph Wedderburn, born in Scotland in 1882, studied at the University of Edinburgh from 1898 to 1903 and received an M.A. degree in math. Between 1903 and 1905 he visited the University of Leipzig, the University of Berlin, and the University of Chicago. He interacted with Ferdinand Frobenius in Germany (we'll see more of him in the next section on Section 7.3. A Theorem of Frobenius) and Leonard Dickson in Chicago (we'll see more of him in Supplement. The Cayley-Dickson Construction and Nonassociative Algebras, a supplement to Section 7.3). These interactions stimulated his interest in algebra and, in particular, the determination of finite division algebras. In 1905 he returned to Scotland and the University of Edinburgh. In the following four years Wedderburn made major contributions to algebra. In a 1905 paper, "A Theorem on Finite Algebras," *Transactions of the American Mathematical Society* **6**, 349–352 (1905) (available online on JSTOR; accessed 11/12/2022), curiously authored by "J. H. Maclagan-Wedderburn" (his full name according to the MacTutor History of Mathematics Archive website is Joseph Henry Maclagen Wedderburn) he gives a proof that a noncommutative finite field can not exist. The implication is that any finite division ring must be commutative and therefore must be a field (*this* is "Wedderburn's Theorem on Finite Division Rings." In fact, Wedderburn gave three proofs. Karen Parshall (in "In Pursuit of the Finite Division Algebra Theorem and Beyond: Joseph H. M. Wedderburn, Leonard E. Dickson and Oswald Veblen," *Archives Internationales d'Histoire des*

Sciences **33**(111), 284–299 (1983)) reviews the work on this result. Quoting from the MacTutor History of Mathematics Archive biography of Wedderburn (accessed 11/12/2022):

> "She notes that the first of the three proofs has a gap in it which was not noticed at the time. This is in fact significant since Dickson also found a proof of this result but, since Wedderburn had already found his first 'proof' (which Dickson believed to be correct), Dickson acknowledged Wedderburn's priority in a paper he wrote on the topic. Dickson noted in the paper that it is only after having seen his proof that Wedderburn constructed his second and third proofs. Parshall's work here shows that really Dickson should be credited with having found the first correct proof."

The paper by Leonard Dickson is "On Finite Algebras," *Nachrichten der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 358-393 (1905) (available online on the European Digital Mathematics Library, accessed 11/12/2022). In 1931, Ernst Witt in "Über die Kommutativität endlicher Schiefkörper,", *Abh. Math. Sem. Univ. Hamburg*, **8**, 413 (1931), gave a simplified proof of Wedderburn's result which has become the standard textbook proof. In fact, it is given in M. Aigner and G. M. Ziegler's *Proofs from THE BOOK*, 6th edition, Springer (2018) as Chapter 6, "Every Finite Division Ring is a Field." A copy of this chapter (from the 3rd edition of the book) is online on Hans Finkelnberg's webpage on the Mathematical Institute of Leiden University website (accessed 11/12/2022). In fact, it is Witt's proof that we give in these notes. Wedderburn published "On Hypercomplex Numbers," *Proceedings of the London Mathematical Society*, 2nd series, **6**, 77–118 (November 1907) (you can download this paper at Semantic Scholar;

accessed 11/12/2022) in which he gave a classification of semisimple algebras. He proved that every semisimple algebra is a direct sum of simple algebras and that a simple algebra was a matrix algebra over a division ring. This is commonly called "Weddeburn's Theorem" or the "Wedderburn-Artin Theorem," and the result on finite division rings is sometimes called "Wedderburn's Little Theorem" (see T. Y. Lam's *A First Course in Noncommutative Rings*, 2nd Edition, Springer, (2001) for more on this). In 1909, Wedderburn took a position at Princeton University. With the outbreak of World War I, he volunteered for the British Army and served until 1919. He returned to Princeton after the war and worked there until taking an early retirement in 1945. Around 1928, he seems to have suffered some mental issues (possibly depression), and became rather isolated (Princeton granting him an early retirement which they deemed to be in his best interest). He died at home (alone) of an apparent heat attack in 1948.

Joseph H. M. Wedderburn (February 2, 1882–October 9, 1948)

This image and these historical notes are from the MacTutor History of Mathematics Archive biography of Wedderburn (accessed 11/11/2022).

Note. A statement of Wedderburn's Theorem on Finite Division Rings is given in the Modern Algebra sequence (MATH 5410, MATH 5420) in Section IX.6, "Division Algebras." The proof which we give below is to be given in Modern Algebra 2 in Section V.8. Cyclotomic Extensions (see Exercise V.8.10 there).

Note. As if from an episode of *Strange But True*, a group theoretic proof of Wedderburn's result was given in Ted Kaczynski, "Another Proof of Wedderburn's Theorem," *American Mathematical Monthly*, **71**(6), 652-653 (June-July 1964). This is available through JSTOR but requires your ETSU username and password to access (accessed 11/12/2022). Ted Kaczynski is better known as the "Unabomber." He is responsible for the killing three people and injuring 23 others in a 1978 to 1995 mail bomb campaign.

Note. Recall that a *division ring* is a ring in which the nonzero elements (that is, the non additive identity elements) form a group under addition. Therefore each nonzero element of a division ring has a multiplicative inverse. We need some additional definitions and results before proving Wedderburn's Theorem on Finite Division Rings.

Note. Consider the polynomial $x^n - 1 \in \mathbb{C}[x]$. Then with $\lambda_1, \lambda_2, \ldots, \lambda_n$ as the distinct complex nth roots of 1, we have $x^n - 1 = \prod_{i=1}^n (x - \lambda_i)$. The nth complex roots of 1 form a multiplicative cyclic group (generated by, for example, $e^{2\pi i/n}$; this is the first example of a group given in Introduction to Modern Algebra [MATH 4127/5127] in Section I.1. Introduction and Examples).

Definition. A *primitive nth root of unity* is $\theta \in \mathbb{C}$ such that $\theta^n = 1$ but $\theta^m \neq 1$ for any positive integer $m < n$. A *cyclotomic polynomial* is one of the form $\Phi_n(x) = \prod(x - \theta)$ where the product is taken over all θ primitive nth roots of 1.

Note 7.2.A. In my online notes for Modern Algebra 2 (MATH 5420) on Section V.8. Cyclotomic Extensions, the following is proved.

> **Proposition V.8.2.** Let n be a positive integer, K a field such that char(K) does not divide n and $\Phi_n(x)$ the nth cyclotomic polynomial over K.
>
> **(i)** $x^n - 1_K = \prod_{d|n} \Phi_n(x)$.
>
> **(ii)** The coefficients of $\Phi_n(x)$ lie in the prime subfield of K. If char$(K) = 0$ and P is identified with the field $\mathbb{Q}$ or rationals, then the coefficients are actually integers.
>
> **(iii)** The degree of $\Phi_n(x)$ is $\phi(n)$, where ϕ is the Euler function.

For details on the Euler function, see my online notes for Elementary Number Theory (MATH 3120) on Section 9. Euler's Theorem and Function. In our case, we have $k = \mathbb{C}$ which is of characteristic 0 and the prime subfield is $P = \mathbb{Q}$ (see Section V.5. Finite Fields of my Modern Algebra 2 online notes), so we can conclude that $x^n - 1 = \prod_{d|n} \Phi_d(x)$ where each $\Phi_d(x)$ is a monic polynomial with integer coefficients.

Note. The first six cyclotomic polynomials are: $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$.

Theorem 7.2.1. **(Wedderburn's Little Theorem)** A finite division ring is necessarily a field.

Note. We now give a second proof of Wedderburn's Theorem on Finite Division Rings. We need some preliminary results before giving the second proof. The advantage of this second proof is that it lets us show that division rings satisfying a certain element-wise identity are commutative (that is, are fields). We see this in Theorem 7.2.2, "Jacobson's Theorem."

Lemma 7.2.1. Let R be a ring and let $a \in R$. Let T_a be the mapping of R into itself defined by $xT_a = xa - ax$ (so xT_a is the commutator of x and a. Then iterating T_a m times gives

$$\begin{aligned} aT_a^m &= xa^m - maxa^{m-1} + \frac{m(m-1)}{2}a^2xa^{m-2} - \frac{m(m-1)(m-2)}{3!}a^3xa^{m-3} + \\ &\quad \cdots + (-1)^{m-1}ma^{m-1}xa + (-1)^m a^m x = \sum_{k=0}^{m} \binom{m}{k}(-1)^k a^k x a^{m-k}. \end{aligned}$$

Corollary 7.2.A. If R is a ring in which $px = 0$ for all $x \in R$, where p is a prime number, then $xT_a^{p^m} = xa^{p^m} - a^{p^m}x$.

Lemma 7.2.2. Let D be a division ring of characteristic $p > 0$ with center Z, and let $P = \{0, 1, 2, \ldots, (p-1)\}$ be the subfield of A isomorphic to J_p. Suppose that $a \in D$, $a \notin Z$ is such that $a^{p^n} = a$ for some $n \geq 1$. Then there exists an $x \in D$ such that

1. $xzx^{-1} \neq a$, and

2. $xax^{-1} \in P(a)$ the field obtained by adjoining a to P.

Corollary 7.2.B. In Lemma 7.2.2, $axa^{-1} = a^i \neq a$ for some integer i.

Note. We now have what we need to give the **second proof of Wedderburn's Little Theorem**.

Theorem 7.2.2. **(Jacobson)** Let D be a division ring such that for every $a \in D$ there exists a positive integer $n(a) > 1$, depending on a, such that $a^{n(a)} = a$. Then D is a commutative field.

Note.

Revised: 1/12/2023