Introduction to Modern Algebra

Section 7.2. Wedderburn's Theorem on Finite Division Rings—Proofs of Theorems

Theorem 7.2.1

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

Proof. Let K be a finite division ring and let $Z = \{z \in K \mid zx = xz \text{ for all} x \in K\}$ be its center. Then Z is a commutative division ring; i.e., Z is a field. Treat K as a vector space over scalar field Z (here, linear combinations in Z are defined as other elements of K; K contains a 0 vector and all the needed distribution, associativity, and commutativity rules apply so that we indeed have a vector space). Every vector space has a basis by the Axiom of Choice (see my online notes for Fundamentals of Functional Analysis [MATH 5740] on Section 5.1. Groups, Fields, and Vector Spaces; notice Theorem 5.1.4), so for some $v_1, v_2, \ldots, v_n \in K$ we have that every element of K has a unique representation in the form $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ where $\alpha_1, \alpha_2, \ldots, \alpha_n \in Z$. So the number of elements in K is determined by the number of possible n-tuples $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ of elements of Z.

Theorem 7.2.1 (continued 1)

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

Proof (continued). Therefore, if Z has q elements, then K has q^n elements. We will show that $n = 1$ and hence $Z = K$ so that K is a field.

For $a \in K$, define $N(a) = \{x \in K \mid xa = ax\}$ (the elements of K that commute with a). Then $N(a)$ contains Z. Notice that for each a, $N(z)$ includes 0 and 1, and is closed under addition and multiplication so that $N(z)$ is a sub-division ring of K. As argued above, we can treat $N(a)$ as a vector space over field Z and so $N(z)$ contains $q^{n(a)}$ elements for some $n(a) \in \mathbb{N}$. Since K and $N(a)$ are division rings, then their nonzero elements form a group under multiplication (of orders $q^n - 1$ and $q^{n(a)} - 1$, respectively). Since $N(a)$ under multiplication is a subgroup of K, then by Lagrange's Theorem we have that $q^{n(a)} - 1$ divides $q^n - 1$. This implies, by Problem 7.2.1, that $n(a)$ divides n.

Theorem 7.2.1 (continued 2)

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

Proof (continued). Recall that the *normalizer* of a in group K is the set $\{x \in K \mid xa = ax\}$ (see Section 2.11. Another Counting Principle). The number of elements in K that are conjugate to a is the index of the normalizer of a in the multiplicative group of nonzero elements of K by Herstein's Theorem 2.11.1; Hungerford calls the set $\{x \in K \mid xa = ax\}$ the *centralizer* of a, and Herstein's Theorem 2.11.1 corresponds to Hungerford's Corollary II.4.4(i) (see Section II.4. The Action of a Group on a Set). The group of nonzero elements of K has $q^n - 1$ elements and the nonzero elements of the centralizer of a has $q^{n(a)} - 1$ elements. Again by Lagrange's Theorem the index is $(q^n - 1)/q^{n(a)} - 1)$ so that this is the number of conjugates of a in K. Now $a \in Z$ (the center of K) if and only if a commutes with all elements of K so that $a \in Z$ if and only if $q^{n(a)} = q^n$ (i.e., $n(a) = n$).

Theorem 7.2.1 (continued 3)

Proof (continued). By the class equation as applied to the groups of nonzero elements of K and $N(a)$ we have

$$\left(\begin{array}{c}\text{Order of group of}\\ \text{nonzero elements of } k\end{array}\right) = \sum \frac{\left(\begin{array}{c}\text{Order of group of}\\ \text{nonzero elements of } k)\end{array}\right)}{(\text{Order of the normalizer of } a)}$$

where the sum runs over one element a of each conjugacy class; this follows from Herstein's Corollary to Theorem 2.11.1, and from Hungerford's Corollary II.4.4(ii) and Lagrange's Theorem. Since the nonzero elements of Z form one conjugacy class of a (the class for which $n(a) = n$), then the equation becomes

$$q^n - 1 = (q-1) + \sum_{n(a)|n,\, n(a)\neq n} \frac{q^n - 1}{q^{n(a)} - 1} \qquad (1)$$

where the sum runs over one element a of each conjugacy class, except for the conjugacy class of the nonzero elements of Z.

Theorem 7.2.1 (continued 4)

Proof (continued). We will show that equation (1) has no integer solution, except when $n = 1$ (s that the summation is not present).

Note. Wedderburn's original paper followed the above approach up to this point. He then used number theoretic results to conclude his proof. Very much to Herstein's credit, he gives an alternative argument so that all steps can be justified.

We'll show the existence of an integer which divides each $(q^n - 1)/(q^{n(a)} - 1)$ for all divisors $n(a)$ of n except $n(a) = n$ (and so divides $q^n - 1$ also) but does not divide $q - 1$. But no such integer can exist, unless $n = 1$ and the sum is not present. We use the theory of cyclotomic polynomials (covered in the problems at the end of Herstein's Section 5.6. The Elements of Galois Theory, in Fraleigh's book in Section IV..23. Factorizations of Polynomials over a Field and Section X.55. Cyclotomic Extensions, and in Hungerford's Section V.8. Cyclotomic Extensions).

Theorem 7.2.1 (continued 5)

Proof (continued). As observed in Notes 7.2.A, we have that the cyclotomic polynomials $\Phi_n(x)$ and the polynomial $x^n - 1 \in \mathbb{C}[x]$ are related as

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \qquad (3)$$

and that each $\Phi_n(x)$ is a monic polynomial with integer coefficients.

We now claim for any divisor d of n where $d \neq n$, that $\Phi_d(x)$ divides $(x^n - 1)/(x^d - 1)$ in the sense that the quotient is a polynomial with integer coefficients. From equation (3) above we have $x^d - 1 = \prod_{k|d} \Phi)k(x)$. Now every divisor of d is also a divisor of n, so from the fact that $x^n - 1 = \prod_{k|n} \Phi_d(x)$ (from equation (3)), we see that we can rearrange some of the $\Phi_d(x)$ to produce $x^d - 1$.

Theorem 7.2.1 (continued 6)

Proof (continued). Explicitly, let $K = \{k_1, k_2, \ldots, k_\ell\}$ where $k_i \in K$ if and only if $k_i \mid d$ and we have

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \prod_{k|n} \Phi(x) = \prod_{k|n, k\in K} \Phi_k(x) \prod_{k|n, k\notin K} \Phi_k(x)$$

$$= \Phi_n(x) \prod_{k|n, k\in K} \Phi_k(x) \prod_{k|n, k\notin K, k\neq n} \Phi_k(x) = \Phi_n(x)(x^d - 1)f(x)$$

where $f(x) = \prod_{k|n, k\in K, k\neq n} \Phi_k(x) = \prod_{k|n, k\nmid d} \Phi_k(x)$. Hence $\Phi_d(x)$ divides $(x^n - 1)/(x^d - 1)$ and the quotient is $f(x)$; since $f(x)$ is a product of cyclotomic polynomials then (by Note 7.2.A) $f(x)$ has integer coefficients, as claimed.

If $t \in \mathbb{Z}$ where $t \neq 1$ then $\Phi_n(x) \in \mathbb{Z}$ and, as just argued, integer $\Phi_n(t)$ divides $(t^n - 1)/(t^d - 1)$ (namely, $f(t)$ times).

Theorem 7.2.1 (continued 7)

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

Proof (continued). Recall equation (1) (where q is the number of elements in the center of the finite division ring):

$$q^n - 1 = (q-1) + \sum_{n(a)|n,\, n(a)\neq n} \frac{q^n-1}{q^{n(a)}-1} \qquad (1)$$

where $n(a)$ is the number of elements in $N(a)$ (the elements of the division ring that commute with a). For $n(a)$ which divide n (the $n(a)$ over which we sum in equation (1)) we have that $\Phi_n(q)$ divides $(q^n-1)/(q^{n(a)}-1)$ (taking $t=q$ and $d=n(a)$ above).

ASSUME $n>1$. We have $\Phi_n(q) = \prod)q-\theta)$ where θ runs over all primitive nth roots of 1. But for all θ an nth primitive root of 1 (notice 1 is not itself a primitive nth root)we have $|q-\theta| > q-1$ by Exercise 7.2.10. Whence $|\Phi_n(q)| = \prod |q-\theta| > q-1$.

Theorem 7.2.1 (continued 8)

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

Proof (continued). But then we cannot have $\Phi_n(q)$ as a divisor of $q-1$, a CONTRADICTION. So the assumption that $n>1$ is false, and hence $n=1$. As described above, with $n=1$ we have that finite division ring K equals its center Z so that K is a commutative division ring. That is, K is a field, as claimed. □

Lemma 7.2.1

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 $xT_a = xa - xa$ (so xT_a is the commutator of x and a. Then iterating T_a m times gives

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

Proof. We give an inductive proof. For the base case $m=1$ we have

$$xT_a^1 = \sum_{k=0}^{1}\binom{1}{k}(-1)^k a^k x a^{1-k} = xa - ax.$$

Lemma 7.2.1 (continued 1)

Proof (continued). Also notice that for $m=2$ we have

$$xT_a^2 = (xa-ax)T_a = (xa-ax)a - a(xa-ax)$$

$$= xa^2 - 2axa + a^2x = \sum_{k=0}^{2}\binom{2}{k}(-1)^k a^k x a^{2-k}.$$

For the induction hypothesis, suppose $m=n$ and

$$xT_a^n = \sum_{k=0}^{n}\binom{n}{k}(-1)^k a^k x a^{n-k}$$

and consider $m=n+1$. We have

$$xT_a^{n+1} = (xT_a^n)T_a = \left(\sum_{k=0}^{n}\binom{n}{k}(-1)^k a^k x a^{n-k}\right) T_a$$

Lemma 7.2.1 (continued 2)

Proof (continued). ...

$$\begin{aligned}
xT_a^{n+1} &= \left(\sum_{k=0}^{n}\binom{n}{k}(-1)^k a^k x a^{n-k}\right) a - a\left(\sum_{k=0}^{n}\binom{n}{k}(-1)^k a^k x a^{n-k}\right) \\
&= \sum_{k=0}^{n}\binom{n}{k}(-1)^k a^k x a^{n-k+1} - \sum_{k=0}^{n}\binom{n}{k}(-1)^k a^{k+1} x a^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}(-1)^k a^k x a^{n-k+1} - \sum_{k=1}^{n}\binom{n}{k-1}(-1)^{k-1} a^k x a^{n-k+1} \\
&\quad -(-1)^n a^{n+1} x \\
&= x a^{n+1} + \sum_{k=1}^{n}\binom{n}{k}(-1)^k a^k x a^{n-k+1} \\
&\quad -\sum_{k=1}^{n}\binom{n}{k-1}(-1)^{k-1} a^k x a^{n-k+1} - (-1)^n a^{n+1} x
\end{aligned}$$

Lemma 7.2.1 (continued 3)

Proof (continued). ...

$$\begin{aligned}
xT_a^{n+1} &= x a^{n+1} + \sum_{k=1}^{n}\left(\binom{n}{k} + \binom{n}{n-1}\right)(-1)^k a^k x a^{n-k+1} \\
&\quad -(-1)^n a^{n+1} x \\
&= x a^{n+1} + \sum_{k=1}^{n}\left(\binom{n+1}{k} + \binom{n}{n-1}\right)(-1)^k a^k x a^{n-k+1} \\
&\quad -(-1)^n a^{n+1} x \text{ since } \binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k} \\
&= \sum_{k=0}^{n}\binom{n+1}{k}(-1)^k a^k x a^{(n+1)-k}.
\end{aligned}$$

So the result holds for $m = n+1$, establishing the induction step. Therefore the equation holds for all $m \in \mathbb{N}$, as claimed. □

Corollary 7.2.A

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 $xT_a^{p^m} = xa^{p^m} - a^{p^m}x$.

Proof. First, consider the prime $p = 2$. By Lemma 7.2.1 we have $xT_a^2 = xa^2 + 2axa - a^2x = xa^2 - a^2x$ since $2axa = 0$. If p is an odd prime, Lemma 7.2.1 gives

$$xT_a^p = \sum_{k=0}^{p}\binom{p}{k}(-1)^k a^k x a^{p-k}.$$

Since p divides $\binom{p}{k} = \dfrac{p(p-1)\cdots(p-k+1)}{k!}$ for all $1 \le k \le p$, then all terms equal zero except for the first and last so that $xT_a^p = xa^p - a^p x$. We give an inductive proof and take these equalities as the base case $m = 1$.

For the induction hypothesis, suppose the result holds for $m = k$ and $xT_a^{p^k} = xa^{p^k} - a^{p^k}x$. ...