WEDDERBURN'S THEOREM AND A THEOREM OF JACOBSON

I. N. HERSTEIN, Cornell University

In teaching an undergraduate class in modern algebra (whose students, although very bright, were mostly sophomores and so had little algebraic knowledge or technique) the author was faced with the problem of presenting to the class two theorems which long had been among his favorites, namely, Wedderburn's theorem on finite division rings and (in the division ring case) Jacobson's theorem that a ring in which $x^{m(x)}=x$ for all x is commutative. In order to do so he devised the proofs presented here; these proofs may be of interest to others confronted with similar problems.

The only facts needed to follow the proofs and which are not absolutely trivial are:

1. The multiplicative group of a finite field is cyclic.

2. If F is a finite field, $\alpha\neq 0\in F$ then there exist λ, $\mu\in F$ so that $1+\lambda^2-\alpha\mu^2=0$.

Of course, many proofs of Wedderburn's theorem exist. In fact, we presented Wedderburn's original proof [2] and the slight twist, in its "punch-line," introduced by Witt [3]. Other proofs, to name but a few, are those of Artin [1] and Zassenhaus [4]. The proof here is closest in spirit to that of Artin, but seems to be both shorter and more elementary. Moreover, no use is made either of counting or of nontrivial number theory. It is of interest that the proof finally hinges on the fact that the quaternions over a finite field do not form a division ring. This is equivalent to making use of fact (2) in the introduction.

We begin with

LEMMA 1. *Let D be a division ring of characteristic $p>0$ with center Z, and P the prime field with p elements contained in Z. Suppose $a\in D$, $a\notin Z$ is such that $a^{p^n}=a$ for some $n>0$. Then there exists an $x\in D$ such that*

(1) $xax^{-1}\neq a$,

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

Proof. Define the mapping $\delta: D\to D$ by $\delta(x)=xa-ax$ for all $x\in D$. $P(a)$ is a finite field, and has, say, p^m elements. These all satisfy the equation $u^{p^m}=u$. By a trivial verification we immediately have that $\delta^p(x)=xa^p-a^px$, $\delta^{p^m}(x)=xa^{p^m}-a^{p^m}x=xa-ax=\delta(x)$ for all $x\in D$. Thus $\delta^{p^m}=\delta$.

Now if $\lambda\in P(a)$, $\delta(\lambda x)=(\lambda x)a-a(\lambda x)=\lambda(xa-ax)=\lambda\delta(x)$ since λ commutes with a. Thus if I denotes the identity map on D, $\delta\lambda I=(\lambda I)\delta$ for all $\lambda\in P(a)$. Now the polynomial $u^{p^m}-u$ considered over $P(a)$ has all its p^m roots as the elements of $P(a)$. Thus $u^{p^m}-u=\prod_{\lambda\in P(a)}(u-\lambda)$. Thus since δ commutes with all λI, $\lambda\in P(a)$,

$$0=\delta^{p^m}-\delta=\prod_{\lambda\in P(a)}(\delta-\lambda I).$$

If for every $\lambda\neq 0\in P(a)$, $\delta-\lambda I$ annihilates no nonzero element in D, then since

$\delta(\delta-\lambda_1 I)\cdots(\delta-\lambda_k I)=0$ we would get that $\delta=0$, that is that $xa-ax=0$ for all $x\in D$, forcing $a\in Z$ contrary to hypothesis. Thus there is a $\lambda\neq 0\in P(a)$ and an $x\neq 0\in D$ so that $(\delta-\lambda I)x=0$; that is $xa-ax=\lambda x$ and so $xax^{-1}=a+\lambda\neq a \in P(a)$, proving the lemma.

COROLLARY. *In Lemma* 1 $xax^{-1}=a^i\neq a$ *for some integer* i.

Proof. Let a be of order s, then in the field $P(a)$ all the roots of the polynomial u^s-1 are $1, a, a^2, \cdots, a^{s-1}$. Since xax^{-1} is in $P(a)$ and is a root of this polynomial, $xax^{-1}=a^i$ follows.

We first prove the

THEOREM (Wedderburn). *A finite division ring is a field.*

Proof. Let D be a finite division ring. We assume the theorem to be true for division rings with fewer elements than D.

We first remark that if $a, b\in D$ are such that $b^t a=ab^t$ but $ab\neq ba$, then $b^t\in Z$. For consider $N(b^t)=\{x\in D \mid xb^t=b^t x\}$. $N(b^t)$ is a subdivision ring of D, so if it were not D it would be commutative. Since $a, b\in N(b^t)$ and these do not commute, it must then be that $N(b^t)=D$.

Pick $a\in D$, $a\notin Z$ such that a minimal positive power of a falls in Z. Clearly this minimal power is a prime, r. By the corollary to Lemma 1, there is an $x\in D$ such that $xax^{-1}=a^i\neq a$. Since r is a prime, using the little Fermat theorem, $x^{r-1}ax^{-(r-1)}=a^{i^{r-1}}=a^{1+ru}=aa^{ru}=\lambda a$ where $a^{ru}=\lambda\in Z$. Since $x\notin Z$, $x^{r-1}\notin Z$ by the minimal nature of r; thus by the remark in the paragraph above, $x^{r-1}a \neq ax^{r-1}$, so that $\lambda\neq 1$. Let $b=x^{r-1}$. Thus $bab^{-1}=\lambda a$; consequently $a^r=ba^r b^{-1} =(bab^{-1})^r=\lambda^r a^r$, forcing $\lambda^r=1$. We claim that if $y\in D$ is such that $y^r=1$ then $y=\lambda^i$, for in the field $Z(y)$ there are at most r roots of the polynomial t^r-1 and these are already given by the powers of λ. Now $b^r=\lambda^r b^r=(a^{-1}ba)^r=a^{-1}b^r a$; thus $b^r a=ab^r$, $ba\neq ab$ which implies that $b^r\in Z$. The multiplicative group of Z is cyclic and is generated by an element γ. Thus $a^r=\gamma^n$, $b^r=\gamma^m$. If $n=kr$ then $(a/\gamma k)^r=1$, which would make $a/\gamma k=\lambda^i$ and would lead to $a\in Z$. Thus $r\nmid n$; similarly $r\nmid m$. Let $a_1=a^m$, $b_1=b^n$. Thus $a_1^r=a^{mr}=\gamma^{mn}=b^{nr}=b^r$ and

$$a_1 b_1 = \mu b_1 a_1 (\mu \neq 1 \in Z) \tag{1}$$

($\mu\neq 1$ since $r\nmid n, m$ so $a_1, b_1\notin Z$) and $\lambda^r=1$. Computing $(b_1^{-1}a_1)^r$ using (1) we arrive at

$$(b_1^{-1}a_1)^r = \mu^{-(1+2+\cdots+(r-1))} b_1^{-r} a_1^r = \mu^{-r(r-1)/2}.$$

If r is odd then since $\mu^r=1$, we have that $(b_1^{-1}a_1)^r=1$. But then $b_1^{-1}a_1=\lambda^i$; and this implies that $a_1b_1=b_1a_1$, a contradiction. Hence if r is odd the theorem is proved.

If $r=2$, then since $\mu^2=1$, $\mu\neq 1$ we have $\mu=-1$. The characteristic must also then be different from 2. Also $\alpha=a_1^2=b_1^2\in Z$, $a_1b_1=-b_1a_1\neq b_1a_1$. In Z there are elements ξ, η so that $1+\xi^2-\alpha\eta^2=0$. But then $(a_1+\xi b_1+\eta a_1 b_1)^2=\alpha(1+\xi^2-\alpha\eta^2)$

$=0$. Being in a division ring this yields $a_1+\xi b_1+\eta a_1 b_1=0$. Thus

$$0 \neq 2a_1^2 = a_1(a_1 + \xi b_1 + \eta a_1 b_1) + (a_1 + \xi b_1 + \eta a_1 b_1)a_1 = 0.$$

This contradiction finishes the proof.

We now proceed to prove the

THEOREM (Jacobson). *Let D be a division ring such that for every $x\in D$ there exists an integer $n(x)>1$ so that $x^{n(x)}=x$. Then D is commutative.*

Proof. For $a\neq 0\in D$, $a^n=a$, $(2a)^m=2a$. Putting $q=(n-1)(m-1)+1$ we have $q>1$, $a^q=a$, $(2a)^q=2a$, so that $(2^q-2)a=0$. Thus D has characteristic $p>0$. If P is the prime field with p elements contained in Z, then $P(a)$ has p^h elements, so that $a^{p^h}=a$. So if $a\notin Z$ the conditions of Lemma 1 are satisfied and so there exists a $b\in D$ such that (1) $bab^{-1}=a^u\neq a$. Suppose $b^{p^k}=b$ and consider

$$W = \left\{x \in D \,\middle|\, x = \sum_{i,j}^{p^h,p^k} p_{ij}a^k b^i,\ p_{ij} \in P\right\}.$$

W is finite, is closed under addition, and by virtue of (1) is closed under multiplication. Thus W is a finite ring and being a subring of the division ring D the two cancellation laws hold so it is a finite division ring. But then it is commutative. Since a, $b\in W$ this forces $ab=ba$, contrary to $a^ub=ba$. This proves the theorem.

References

1. Emil Artin, Über einen Satz von Herrn J. H. MacLaglan-Wedderburn, Abh. Math. Sem. Univ. Hamburg, vol. 5, 1927, pp. 245–250.

2. J. H. M. Wedderburn, A theorem on finite algebras, Trans. Amer. Math. Soc., vol. 6, 1905, pp. 349–352.

3. Ernst Witt, Über die Kommutativität endlicher Schiefkörper, Abh. Math. Sem. Univ. Hamburg, vol. 8, 1931, p. 413.

4. Hans Zassenhaus, A group-theoretic proof of a theorem of MacLaglan-Wedderburn, Proc. Glasgow Math. Assoc., vol. 1, 1952, pp. 53–63.

A NOTE ON THE GENERALIZED WILSON'S THEOREM

L. CARLITZ, Duke University

It is familiar that if $m\geqq 1$ and W_m denotes the product of the integers $\leqq m$ and prime to m then ([2], Ths. 47, 59)

$$W_m \equiv \pm 1 \pmod{m}, \tag{1}$$

where the lower sign occurs provided $m=1, 2, 4, p^r, 2p^r$ $(r\geqq 1)$ and p is a prime >2. (For other references see [1], Ch. 3.)

In this note we prove the following related result.

Let p be a fixed prime >3 and let P_m denote the product of the integers $\leqq m$ and prime to p. Then if $p^r \mid m$, $r\geqq 1$, we have

$$P_m \equiv ((p-1)!)^{m/p} \pmod{p^{r+2}} \qquad (p>3). \tag{2}$$