A GROUP-THEORETIC PROOF OF A THEOREM OF MACLAGAN-WEDDERBURN

by HANS J. ZASSENHAUS

(Received 5th February, 1951)

The purpose of this paper is to present a proof of the following theorem of Maclagan-Wedderburn.*

Every finite skew-field† *is a field.*

The proof depends on group theory and on the properties of Galois fields. As an introduction, §§1–4 are devoted to a systematic and self-contained account of the theory of Galois fields.

§1. *Determination of all Galois Fields.*

Definition: A finite field, i.e., a field with only a finite number of elements, is called a *Galois field.*

This name has been given to such fields because Galois was the first to publish‡ investigations concerning finite fields, though the idea of using finite fields to describe the procedures involved in the solution of higher congruences

$$f(x) \equiv 0 \ (p),$$

where $f(x)$ is a polynomial with integral coefficients and p is a prime number, was probably familiar to Gauss before Galois had published his papers.

Let F be a Galois field with q elements. Since F has only a finite number of elements, its characteristic is a prime number p, and its prime field is a field F_p isomorphic with the field of residue classes of the rational integers modulo p.

The field F, considered as an extension of F_p, is a linear space over F_p. This linear space is of finite dimensions, for it is spanned by the set of all q elements of F. Let the dimension of this linear space be r; then there is a set of r linearly independent elements of F, $a_1, a_2, \ldots, a_r$, say, and every element of F is of the form

$$\xi_1 a_1 + \xi_2 a_2 + \ldots \quad + \xi_r a_r, \quad (\xi_1, \xi_2, \ldots, \xi_r \epsilon F_p).$$

Since each coefficient ξ_i can be any one of the p elements of F_p, it follows that there are p^r elements in F:

$$q = p^r.$$

The multiplicative group of the non-zero elements of F has order $q-1$. Hence, by Fermat's theorem, each non-zero element of F satisfies the equation

$$x^{q-1} = 1,$$

where 1 is the unity element of F and therefore of F_p. Hence each non-zero element of F satisfies the equation

$$x^q = x.$$

* A Theorem on Finite Algebras. American M. S. Transactions, 6, pp. 349–352, (1905).

† A skew-field or division ring is an algebraic system which satisfies all the postulates of a field except possibly that which demands that multiplication shall be commutative ; i.e., it is a ring, not necessarily commutative, whose non-zero elements form a multiplicative group. The theorem states that if the number of elements is finite, the commutative property of multiplication is a consequence of the other postulates.

‡ *Liouville's Journal* XI (1846), pp. 381–444.

https://doi.org/10.1017/S2040618500035474 Published online by Cambridge University Press

Since the zero element 0 of F also satisfies this equation, it follows that the q elements of F are q distinct zeros of the polynomial $t^q - t$ and therefore that

$$t^q - t = \prod_{a \in F} (t - a).$$

Thus F is a splitting field of the polynomial $t^q - t$. Since F contains no other elements than the zeros of the polynomial, it is a minimal splitting field of F over F_p (the smallest field which contains the coefficients of the polynomial).

Conversely, let $q = p^r$ be any power of a prime number p. Let F_p be a prime field of p elements and let F be a minimal splitting field of the polynomial $t^q - t$ over F_p. Let

$$t^q - t = \prod_{i=1}^{q} (t - a_i), \quad a_i \in F.$$

Since $a_i{}^q = a_i$, we have

$$\begin{aligned} t^q - t &= t^q - t - a_i{}^q + a_i \\ &= (t^q - a_i{}^q) - (t - a_i) \\ &= (t - a_i)^q - (t - a_i) \\ &= (t - a_i)\{(t - a_i)^{q-1} - 1\}. \end{aligned}$$

Hence $(t - a_i)^2$ is not a factor of $t^q - t$; i.e., the zeros of $t^q - t$ are all distinct. They form a subset of F which is closed under addition, since

$$(a_i + a_j)^q = a_i{}^q + a_j{}^q = a_i + a_j,$$

and the set of whose non-zero elements is closed under multiplication, since

$$(a_i a_j)^q = a_i{}^q a_j{}^q = a_i a_j.$$

Hence, by Euler's Theorem, this subset of elements of F forms a subfield of F. This subfield of F contains F_p and is a splitting field of $t^q - t$; since F is a minimal splitting field of this polynomial over F_p, it follows that the subfield is F itself, i.e., that F is the set $a_1, a_2, \ldots, a_q$ of zeros of $t^q - t$.

The results established so far may be summarised in

Theorem 1. *The number of elements in any Galois field is equal to a power p^r of its characteristic, the prime number p. For each power p^r of any prime number p, there is a Galois field of p^r elements; this Galois field is determined up to isomorphism as a minimal splitting field of the polynomial $t^q - t$, where $q = p^r$, over the prime field F_p.*

We denote the Galois field of p^r elements by $GF(p^r)$. In this notation, F_p is $GF(p)$.

We now prove

Theorem 2. *The multiplicative group of a Galois field is cyclical.*

This theorem follows immediately from the following purely group-theoretic theorem, stating a characteristic property of finite cyclical groups.

Any finite group G in which, for all positive integral values of n, the equation

$$x^n = 1,$$

where 1 is the identity element of G, has at most n solutions, is cyclical.

Proof. Let G have order N. Then any element of G has an order d which is a factor of N. For each factor d of N, let $\alpha(d)$ be the numbers of element of G of order d; then

$$N = \sum_{1 \leqslant d \leqslant N} \alpha(d).$$

Similarly, if $\beta(d)$ is the number of elements of order d of the cyclical group G', say, of order N, then

$$N = \sum_{1 \leqslant d \leqslant N} \beta(d).$$

https://doi.org/10.1017/S2040618500035474 Published online by Cambridge University Press

We have to show that $\alpha(N)>0$. Since G' is generated by an element a, say, of order N, $\beta(N)>0$. It will therefore be sufficient to show that $\alpha(N)\geqslant\beta(N)$.

If for a particular factor d of N, $\alpha(d)>0$, G has an element y, say, of order d. This element generates a subgroup (y) of G, all of whose elements $y, y^2, \ldots, y^{d-1}, 1$ satisfy the equation

$$x^d=1.$$

Since this equation has, by hypothesis, not more than d solutions, and since each element of G of order d satisfies it, it follows that all the $\alpha(d)$ elements of G of order d are in the subgroup (y). Now G' has a subgroup isomorphic with (y), viz., the subgroup generated by $a^{N/d}$. The elements of this subgroup have the same order as the corresponding elements of (y) ; so this subgroup of G' contains $\alpha(d)$ elements of order d. Hence, if $\alpha(d)>0$, $\beta(d)\geqslant\alpha(d)$. This inequality is obviously also true if $\alpha(d)=0$. Thus

$$\alpha(N)=N-\sum_{1\leqslant d<N}\alpha(d)\geqslant N-\sum_{1\leqslant d<N}\beta(d)=\beta(N)>0.$$

This proves the theorem on finite groups.

Since, in a field, an equation of degree n never has more than n solutions, theorem 2 follows immediately.

§ 2. *Subfields of the Galois Field $GF(p^r)$.*

The number of elements in any subfield F of $GF(p^r)$ is of the form p^s, where $0<s\leqslant r$. We now show that s is a factor of r.

Let $r=as+b$, where $0\leqslant b<r$, be the result of division with remainder of r by s. If x is any element of F, then $x^{p^s}=x$; hence $x^{p^{2s}}=(x^{p^s})^{p^s}=x^{p^s}=x$, and, by induction $x^{p^{ms}}=x$, where m is any integer ; in particular, $x^{p^{as}}=x$. Thus, since x is an element of $GF(p^r)$,

$$x=x^{p^r}=(x^{p^{as}})^{p^b}=x^{p^b}.$$

Hence if $0<b<s$, the equation $x^{p^b}=x$ has at least p^s and therefore more than p^b solutions, which is impossible. Hence $b=0$, i.e., $r=as$, i.e., s is a factor of r.

Since each element of F satisfies the equation

$$x^{p^s}=x,$$

so that F supplies p^s distinct roots of this equation, and since F has no elements other than the roots of this equation, it follows that F is uniquely determined as the minimal splitting field of the polynomial $t^{p^s}-t$ in $GF(p^r)$.

Conversely, let s be any factor of r and let $r=ds$. Let F^* be a splitting field of $t^{p^s}-t$ ove $GF(p^r)$, so that

$$t^{p^s}-t=\prod_{i=1}^{p^s}(t-a_i),\quad a_i\epsilon F^*.$$

Hence $a_i{}^{p^s}=a_i$ and therefore, as in an earlier argument,

$$a_i{}^{p^{ds}}=a_i,\quad \text{i.e.,}\quad a_i{}^{p^r}=a_i$$

and consequently a_i is in $GF(p^r)$. Hence $GF(p^r)$ already contains a splitting field of $t^{p^s}-t$, consisting of the zeros of this polynomial. Since this splitting field contains only these zeros, it is a minimal splitting field of this polynomial, over the prime field F_p of $GF(p^r)$, (F_p being the smallest subfield of $GF(p^r)$ which contains the coefficients of the polynomial). We thus have

THEOREM 3. *A Galois field $GF(p^r)$ of p^r elements and characteristic p contains, for each factor s of r, one and only one subfield of p^s elements, the elements of this subfield being the zeros of the polynomial $t^{p^s}-t$ in $GF(p^r)$. There are no other subfields.*

https://doi.org/10.1017/S2040618500035474 Published online by Cambridge University Press

§ 3. *Automorphisms of the Galois Field GF* (p^r).

We first observe that in any field F of characteristic p, the correspondence σ which maps each element x of F on the element x^p is an automorphism. In the first place, the correspondence is one-one, for if x and y are any elements of F,

$$(x-y)^p = x^p - y^p,$$

and therefore $x^p = y^p$ if and only if $x = y$. In the second place, the correspondence preserves addition and multiplication, for

$$(x+y)^p = x^p + y^p$$

and $$(xy)^p = x^p y^p$$

The correspondence is therefore an automorphism. We write it in the form $x \to x^\sigma$.

The result of ν applications, where ν is any positive integer, of the automorphism is an automorphism σ^ν under which the image of each element x of F is its p^ν-th power. The automorphisms σ^ν of F form a cyclical group (σ) generated by σ.

If the field under consideration is $GF(p^r)$, then

$$x^{\sigma^r} = x^{p^r} = x\,;$$

the automorphism σ^r is therefore the identity. On the other hand, if $0 < \nu < r$, the equation

$$x^{\sigma^\nu} = x, \quad \text{i.e.,} \quad x^{p^\nu} = x$$

is not satisfied by all the $p^r (> p^\nu)$ elements of $GF(p^r)$. Hence the automorphism σ^ν is not the identity. The cyclical group (σ) is therefore of order r.

If s is a factor of r, say $r = ds$, there is, as we have already seen, a subfield $GF(p^s)$ of $GF(p^r)$ consisting of the p^s roots of the equation

$$x^{p^s} = x$$

in $GF(p^r)$. The elements of this subfield are therefore left invariant by σ^s and all its powers. Conversely, if σ^ν leaves each element of $GF(p^s)$ invariant, and if $\nu = as + b$, where $0 \leqslant b < s$, we have

$$x = x^{\sigma^\nu} = x^{p^\nu} = (x^{p^{as}})^{p^b} = x^{p^b},$$

for all x in $GF(p^s)$. If $0 < b < s$, this would mean that the polynomial $t^{p^b} - t$ had more than p^b zeros, which is impossible. Hence $\nu = as$, and therefore $\sigma^\nu = \sigma^{as}$.

Thus the set of all powers of σ which leave each element of $GF(p^s)$ invariant forms a subgroup (σ^s) of (σ) of order d and index s; and $GF(p^s)$ consists of all elements of $GF(p^r)$ left invariant by σ^s, and therefore by all its powers.

We now show that there is no automorphism of $GF(p^r)$ other than the powers of σ. If there is any automorphism which is not a power of σ, let τ be one of those which leave invariant a maximum number of elements of $GF(p^r)$. The set of all elements left invariant by τ forms a subfield; for if τ is written in the form $x \to x^\tau$ and if a and b are any elements of $GF(p^r)$ left invariant by τ, then $a^\tau = a$ and $b^\tau = b$ and therefore

$$(a+b)^\tau = a^\tau + b^\tau = a + b$$

and $$(ab)^\tau = a^\tau b^\tau = ab.$$

Thus the set is closed under addition and multiplication; and it includes the zero and the unity of $GF(p^r)$. Hence it forms a subfield, which must be one of the subfields $GF(p^s)$, where s is a factor of r.

Since τ is not the identity, which is σ^r, it follows that there is an element in $GF(p^r)$ but not in $GF(p^s)$. Let x be such an element and consider the polynomial

$$f(t) = \prod_{i=1}^{d} (t - x^{p^{is}}).$$

https://doi.org/10.1017/S2040618500035474 Published online by Cambridge University Press

The application of σ^s to the coefficients of this polynomial produces the polynomial

$$\prod_{i=1}^{d}\{t-(x^{p^{is}})^{p^s}\},\quad \text{i.e.,}\quad \prod_{i=1}^{d}\{t-x^{p^{(i+1)s}}\},\quad \text{i.e.,}\quad \prod_{i=1}^{d}\{t-x^{p^{is}}\},$$

since $x^{p^{(d+1)s}}=(x^{p^{ds}})^{p^s}=x^{p^s}$; i.e., it produces $f(t)$. Thus all the coefficients of $f(t)$ lie in $GF(p^s)$. They are therefore left invariant by τ. On the other hand the application of τ to the coefficients of $f(t)$ produces

$$\prod_{i=1}^{d}\{t-(x^{p^{is}})^{\tau}\},$$

the last factor of which is $t-x^{\tau}$. Hence x^{τ} must be one of the powers $x^{p^{is}}$, say $x^{p^{js}}$, i.e., $x^{\sigma^{js}}$. Thus the automorphism $\tau\sigma^{-js}$ leaves invariant each element of $GF(p^s)$, and also the element x which is not in $GF(p^s)$, i.e., it leaves invariant more elements than τ. On the other hand it does not belong to (σ). This contradicts the maximum property of τ. It follows that there is no automorphism of $GF(p^r)$ which is not a power of σ.

These properties of the automorphisms of $GF(p^r)$ are collected in

THEOREM 4. *The automorphisms of the Galois field $GF(p^r)$ of p^r elements and characteristic p form a cyclical group (σ) of order r generated by the automorphism σ defined by*

$$x\rightarrow x^p=x^{\sigma}.$$

The set of automorphisms which leave invariant each element of the subfield $GF(p^s)$, where $r=ds$, forms a subgroup (σ^s), of order d and index s, generated by σ^s, of the full group of automorphisms.

Conversely, each subgroup of (σ) is generated by some σ^s, where s is a factor of r, and the set of elements of $GF(p^r)$ left invariant by each automorphism of the subgroup (σ^s) forms the subfield $GF(p^s)$ of $GF(p^r)$.

§ 4. *Norms in Galois Fields.*

Let F be the Galois field $GF(p^r)$ and let S be its subfield $GF(p^s)$, where $r=ds$. The group (σ^s) of automorphisms of F which leave invariant each element of S is called the group of automorphisms of F over S and is denoted by $G_{F/S}$. Its order $G_{F/S}:1$ is d. If $q=p^s$, the number of elements in S, then the number of elements in F is $p^r=p^{ds}=q^d$.

For any element x of F, we define its *conjugates over* S to be the d elements x^{τ}, where τ is in $G_{F/S}$; these d elements need not all be distinct. All the distinct conjugates of x appear in the set of all its d conjugates with the same multiplicity; for if $x^{\tau}=x^{\tau'}$, then $x^{\rho\tau}=x^{\rho\tau'}$, where $x^{\rho\tau}$ means $(x^{\tau})^{\rho}$, and conversely.

The product of all the d conjugates of x over S is called the *norm* of x over S and is denoted by $N_{F/S}(x)$:

$$N_{F/S}(x)=\prod_{\tau\epsilon G_{F/S}} x^{\tau}.$$

Since any automorphism of F over S simply permutes the conjugates of x over S, $N_{F/S}$ is left invariant by each such automorphism and is therefore an element of S:

$$N_{F/S}(x)\epsilon S.$$

The norm has also the following easily verified properties:

$$N_{F/S}(xy)=N_{F/S}(x)\,N_{F/S}(y),$$
$$N_{F/S}(\xi)=\xi^{G_{F/S}:1},\quad \text{if } \xi\epsilon S.$$

The group $G_{F/S}$ consists of the automorphisms

$$x\rightarrow x^{p^{ms}},\quad (x\epsilon F\,;\ m=0,1,2,\ldots,d-1),$$

i.e.,

$$x\rightarrow x^{q^m},\quad (m=0,1,2,\ldots,d-1).$$

https://doi.org/10.1017/S2040618500035474 Published online by Cambridge University Press

Hence $$N_{F/S}(x)=x^{1+q+q^2+\dots+q^{d-1}}=x^{(q^d-1)/(q-1)}. \qquad\dots\dots(1)$$

We now prove

THEOREM 5. *Each element of any subfield S of a Galois field F is the norm over S of some element of F.*

Proof. The correspondence which maps each non-zero element of F on its norm over S is a homomorphism of F', the multiplicative group of F, onto a subgroup of F'. The kernel of this homomorphism is the set of elements of x whose norms are 1, the unity of F, i.e., the set of elements x of F for which

$$x^{(q^d-1)/(q-1)}=1.$$

Since F is a field, there cannot be more than $(q^d-1)/(q-1)$ such elements. Since F' has q^d-1 elements, it follows that the factor group of F' over the kernel has at least

$$(q^d-1)/\{(q^d-1)/(q-1)\},$$

i.e., $(q-1)$ elements. But the set of non-zero norms, being the image of F' under the homomorphism, is isomorphic with this factor group ; the number of distinct non-zero norms is therefore also at least $(q-1)$. On the other hand, since each norm is a non-zero element of S, there are at most $(q-1)$ distinct non-zero norms. Hence there are exactly $(q-1)$ non-zero norms ; i.e., each non-zero element of S is the norm of some element of F. The zero of S is the norm of the zero element of F.

This completes the proof.

We now prove the further theorem

THEOREM 6. *If S is a subfield with q elements of a Galois field F with q^d elements, then each element x of F whose norm over S is 1 is of the form*

$$x=y^{q-1} \quad (y\epsilon F),$$

and conversely.

Proof. If $x=y^{q-1}$, then, by (1),

$$N_{F/S}(x)=y^{q^d-1}=y^{q^d}y^{-1}=yy^{-1}=1.$$

This establishes the converse part of the theorem.

To prove the direct part, we observe that the correspondence

$$y\rightarrow y^{q-1} \quad (y\epsilon F')$$

is a homomorphism of F' onto a subgroup of F'. The kernel of this homomorphism is the set of elements of y of F for which $y^{q-1}=1$. Since F is a field this equation has not more than $q-1$ solutions. The kernel has therefore at most $q-1$ elements and consequently the factor-group of F' over the kernel has order at least $(q^d-1)/(q-1)$. But the set of elements of the form y^{q-1}, being the image of F' under the homomorphism, is isomorphic with this factor-group. It follows that there are at least $(q^d-1)/(q-1)$ elements of F of the form y^{q-1}. On the other hand, since each element of the form y^{q-1} satisfies the equation (1), there are at most $(q^d-1)/(q-1)$ such elements. It follows that there are exactly $(q^d-1)/(q-1)$ elements of this form. Since the equation (1) has these as solutions and cannot have more than this number of solutions, it follows that the elements y^{q-1} consist of all the solutions of this equation, i.e., they consist of all the elements whose norms are 1.

§ 5. *Proof of Maclagan-Wedderburn's Theorem.*

Let K be a finite skew-field. We have to show that K is a field, i.e., that the multiplicative group K' of the non-zero elements of K is Abelian. The proof depends on the following

https://doi.org/10.1017/S2040618500035474 Published online by Cambridge University Press

LEMMA. *If G is any Abelian subgroup of K', the normaliser of G coincides with the centraliser of G.*

Proof. We have to show that if x is any element of K' satisfying the condition

$$xGx^{-1} = G, \quad \text{.......................}(1)$$

then x also satisfies the condition

$$xax^{-1} = a, \quad \text{for all } a \epsilon G. \quad \text{.......................}(2)$$

Let x be any element satisfying the condition (1). Since, by Fermat's Theorem for the group K',

$$x^{K':1} = 1,$$

and since 1 lies in the centraliser of G, it follows that there is a positive integer μ (viz., $\mu = K' : 1$) for which x^{μ} is in the centraliser of G. Let m be the least positive integer μ for which this is the case. Then

$$x^m a x^{-m} = a; \quad \text{for all } a \epsilon G;$$

but, for each positive integer ν such that $0 < \nu < m$, there is an $a_{\nu} \epsilon G$ for which

$$x^{\nu} a_{\nu} x^{-\nu} \neq a_{\nu}. \quad \text{.......................}(3)$$

Let H be the subgroup of K' generated by x^m and G. Since any two generators of H commute, H is Abelian. Since $xGx^{-1} = G$ and $xx^m x^{-1} = x^m$,

$$xHx^{-1} = H.$$

Let F be the set of all elements of K which are the sums of finite numbers of elements of H, i.e., all elements of the form

$$\sum_{i=1}^{r} b_i \quad (b_i \epsilon H),$$

together with the zero element of K. It is obvious that F is closed under addition; its elements therefore form a subgroup of the additive group of K. It is easily verified that the set of non-zero elements of F is closed under multiplication and therefore forms a subgroup of K'. Finally, since H is Abelian, multiplication in F is commutative. It follows that the set F forms a field.

Since $xHx^{-1} = H$ and $x0x^{-1} = 0$, it follows that, if $y \epsilon F$, then $xyx^{-1} \epsilon F$ and every element of F is of the form xyx^{-1}, where $y \epsilon F$; hence $xFx^{-1} = F$. Further, since

$$x(a+b)x^{-1} = xax^{-1} + xbx^{-1}$$

and

$$x(ab)x^{-1} = (xax^{-1})(xbx^{-1}),$$

the one-one correspondence σ defined by

$$a \rightarrow xax^{-1} = a^{\sigma} \quad (a \epsilon F)$$

is an automorphism of F.

We show that if m, defined earlier, is assumed to be greater than 1, we are led to a contradiction.

Assume, then, that $m > 1$; then

$$a^{\sigma^m} = x^m a x^{-m} = a, \text{ for all } a \epsilon F,$$

but, if $0 < \nu < m$, there is an a_{ν} in G, and therefore in F, for which

$$a_{\nu}^{\sigma^{\nu}} = x^{\nu} a_{\nu} x^{-\nu} \neq a_{\nu}.$$

Thus the automorphism σ^m of F is the identity, but the automorphism σ^{ν}, where $0 < \nu < m$, is not. Consequently σ is an automorphism of F of order m.

https://doi.org/10.1017/S2040618500035474 Published online by Cambridge University Press

Since $(x^m)^\sigma = xx^mx^{-1} = x^m$, x^m is one of the elements left invariant by σ; x^m therefore belongs to the subfield S of F consisting of those elements of F which are left invariant by σ. By theorem 5, therefore, x^m is the norm $N_{F/S}(y)$, over S, of some element y of F; i.e.,

$$x^m = yy^\sigma y^{\sigma^2} \dots y^{\sigma^{m-1}}, \quad (y \epsilon F). \quad \dots\dots(4)$$

For this y, consider the expression

$$(x-y)(1 + y^{-1}x + y^{-1}y^{-\sigma}x^2 + \dots + y^{-1}y^{-\sigma} \dots y^{-\sigma^{m-2}}x^{m-1}).$$

Let us denote it by $f(x, y)$; then

$$\begin{aligned} f(x, y) = x + xy^{-1}x + xy^{-1}y^{-\sigma}x^2 + \dots + xy^{-1}y^{-\sigma} \dots y^{-\sigma^{m-2}}x^{m-1} \\ - y - x - y^{-\sigma}x^2 - \dots - y^{-\sigma}y^{-\sigma^2} \dots y^{-\sigma^{m-2}}x^{m-1}. \end{aligned}$$

Now, in the expression on the right, each term (except the last) in the first row is equal to the term in the succeeding place in the next row; for

$$\begin{aligned} &xy^{-1}y^{-\sigma} \dots y^{-\sigma^{r-2}}x^{r-1} \\ &= (xy^{-1}x^{-1})(xy^{-\sigma}x^{-1}) \dots (xy^{-\sigma^{r-2}}x^{-1})x^r \\ &= y^{-\sigma}y^{-\sigma^2} \dots y^{-\sigma^{r-1}}x^r. \end{aligned}$$

Hence, applying this formula to the last term in the first row also,

$$\begin{aligned} f(x, y) &= -y + y^{-\sigma}y^{-\sigma^2} \dots y^{-\sigma^{m-1}}x^m \\ &= -y + y^{-\sigma}y^{-\sigma^2} \dots y^{-\sigma^{r-1}}yy^\sigma \dots y^{\sigma^{m-1}}, \quad \text{by (4)}, \\ &= -y + y, \end{aligned}$$

since $y, y^\sigma, \dots y^{\sigma^{m-1}}$, being elements of F, commute with one another. Thus $f(x, y) = 0$ and therefore either $x = y$ or

$$1 + y^{-1}x + y^{-1}y^{-\sigma}x^2 + \dots + y^{-1}y^{-\sigma} \dots y^{-\sigma^{m-2}}x^{m-1} = 0. \quad \dots\dots(5)$$

Consider the latter possibility. If (3) holds, then there will be, among the relations of the form

$$1 + \sum_{\nu=1}^{t} c_{j_\nu}x^{j_\nu} = 0, \quad \dots\dots(6)$$

where $0 < j_1 < j_2 < \dots < j_t < m$ and $0 \neq c_{i_\nu} \epsilon F$, one or more relations with t a minimum; let (6) be one such. If, in (6), we multiply on the left by $a_{j_1}^{-1}$, and on the right by a_{j_1}, where a_{j_1} is the element of G, and therefore of F, introduced earlier (see (3)), such that $x^{j_1}a_{j_1}x^{-j_1} \neq a_{j_1}$, we obtain

$$\begin{aligned} 0 &= 1 + \sum_{\nu=1}^{t} a_{j_1}^{-1}c_{j_\nu}x^{j_\nu}a_{j_1} \\ &= 1 + \sum_{\nu=1}^{t} a_{j_1}^{-1}c_{j_\nu}(x^{j_\nu}a_{j_1}x^{-j_\nu})x^{j_\nu} \\ &= 1 + \sum_{\nu=1}^{t} d_{i_\nu}x^{j_\nu}, \quad \dots\dots(7) \end{aligned}$$

say. Since σ and therefore σ^{j_ν} leaves F invariant, $x^{j_\nu}a^{-1}x^{-j_\nu}$ is in F, and therefore d_{j_ν} is in F. Subtracting (7) from (6), and multiplying on the right by x^{-j_1}, we obtain

$$c_{j_1} - d_{j_1} + \sum_{\nu=2}^{t} (c_{j_\nu} - d_{j_\nu})x^{j_\nu - j_1} = 0. \quad \dots\dots(8)$$

Now $c_{j_1} - d_{j_1} \neq 0$, for

$$d_{j_1} = a_{j_1}^{-1}c_{j_1}(x^{j_1}a_{j_1}x^{-j_1}) \neq a_{j_1}^{-1}c_{j_1}a_{j_1} = c_{j_1}a_{j_1}^{-1}a_{j_1} = c_{j_1}.$$

https://doi.org/10.1017/S2040618500035474 Published online by Cambridge University Press

Hence there is an element $(c_{j_1}-d_{j_1})^{-1}$ of F. Multiplying (8) by this on the left, we obtain a relation

$$1+\sum_{\nu=2}^{t} e_{j_\nu} x^{j_\nu - j_1}=0, \quad (e_{j_\nu} \epsilon F),$$

which is of the form (6) but has at least one term fewer, contrary to the supposition that t was a minimum. Thus the assumption that (5) holds leads to a contradiction and we must conclude that $x=y$, and therefore that x lies in F, from which it follows that $xax^{-1}=a$, for all a in F. But this contradicts the assumption that $m>1$. Hence the assumption that $m>1$ leads to a contradiction, and we must conclude that $m=1$; i.e., that any element x which lies in the normaliser of G also lies in the centraliser of G.

This concludes the proof of the Lemma.

The proof of Maclagan-Wedderburn's theorem is now completed by establishing

THEOREM 7. *If, in a finite group G, the normaliser of every Abelian subgroup coincides with the centraliser of that subgroup, then the group G is Abelian.*

We prove this theorem by induction over N, the order of the group G.

If $N=1$, the theorem is obvious.

Let us make the induction hypothesis that the theorem is valid for groups of all orders less than N, and let G be a group of order N possessing the property that the normaliser of each Abelian subgroup of G is also the centraliser of this subgroup. Then any proper subgroup of G also possesses this property and has order less than N; hence by the induction hypothesis, any proper subgroup of G is Abelian.

Let Z be the centre of G, and consider first the case in which Z is not the identity. Then the factor group G/Z has order less than N. We show that, on the induction hypothesis, it is Abelian. If G/Z is not Abelian, let $\bar{U}$ be an Abelian subgroup of G/Z and let $\bar{X}$ be any element of the normaliser of $\bar{U}$, i.e., any element of G/Z such that $\bar{X}\bar{U}\bar{X}^{-1}=\bar{U}$. Let U be the subgroup of G formed by the elements of G in those cosets of Z which form $\bar{U}$. Since $\bar{U}$ is Abelian and G/Z is not, $\bar{U}$ is a proper subgroup of G/Z and therefore U is a proper subgroup of G; hence, as a consequence of the induction hypothesis, U is Abelian. Since $\bar{X}\bar{U}\bar{X}^{-1}=\bar{U}$, it follows that, if x is any element of $\bar{X}$, $xUx^{-1}=U$, i.e., x belongs to the normaliser of U in G and therefore to the centraliser of U in G; i.e., x commutes with every element of U. It follows that $\bar{X}$ commutes with every element of $\bar{U}$, i.e., that $\bar{X}$ belongs to the centraliser of $\bar{U}$. Hence the factor group G/Z satisfies the conditions of the theorem; and it has order less than N. It is therefore, by the induction hypothesis, Abelian. Thus the assumption that G/Z is not Abelian leads to a contradiction, and we conclude that (on the induction hypothesis) G/Z is Abelian.

Let a and b be any two elements of G. Since $bz=zb$ for all elements z of Z and Z is Abelian, the subgroup $\langle b, Z\rangle$ generated by b and Z is Abelian. Since G/Z is Abelian, $aba^{-1}\equiv b(Z)$. Since, in addition, $az=za$ for all z in Z,

$$a\langle b, Z\rangle a^{-1}=\langle b, Z\rangle,$$

i.e., a is in the normaliser of $\langle b, Z\rangle$; it is therefore in the centraliser of $\langle b, Z\rangle$, i.e., it commutes with each element of $\langle b, Z\rangle$. In particular, it commutes with b, i.e.,

$$ab=ba.$$

Hence G is Abelian.

This completes the proof by induction of the theorem, for groups G for which the centre Z is not the identity.

Now consider the case in which Z is the identity. We have already observed that for any group G of order N which satisfies the conditions of the theorem, it follows from the induction

https://doi.org/10.1017/S2040618500035474 Published online by Cambridge University Press

hypothesis that any proper subgroup of G is Abelian. As a consequence of this, if U_1 and U_2 are any two distinct maximal proper subgroups of G, their intersection lies in the centre Z of G. To prove this we observe firstly that the subgroup $\langle U_1, U_2\rangle$ generated by U_1 and U_2 is G itself; and secondly that any element z in the intersection of U_1 and U_2 commutes with each element of U_1 and each element of U_2 and therefore with each element of $\langle U_1, U_2\rangle$, i.e., with each element of G. Thus, in the case under consideration, any two distinct maximal proper subgroups intersect in the identity.

Now let U be any maximal proper subgroup of G. Then any conjugate subgroup xUx^{-1}, where $x\epsilon G$, of U in G is also a maximal proper subgroup of G. We find the condition that two of these conjugate subgroups xUx^{-1} and yUy^{-1} shall coincide.

If
$$xUx^{-1}=yUy^{-1},$$
then
$$(y^{-1}x)U(y^{-1}x)=U.$$
Hence $y^{-1}x$ is in the normaliser of U and therefore, since U is Abelian, in the centraliser of U; i.e., $y^{-1}x$ commutes with every element of U. It therefore commutes with every element of the subgroup $\langle y^{-1}x, U\rangle$. If $y^{-1}x$ is not in U, this new subgroup is G itself; hence $y^{-1}x$ commutes with every element of G, i.e., it is in the centre of G, i.e., it is the identity, and is therefore in U. Thus the assumption that $y^{-1}x$ is not in U leads to a contradiction and we must conclude that $y^{-1}x$ is in U.

Thus if $xUx^{-1}=yUy^{-1}$, $y^{-1}x\epsilon U$. The converse is obviously the case. Hence $xUx^{-1}=yUy^{-1}$ if and only if $x\epsilon yU$, i.e., if and only if $xU=yU$. Hence U has the same number of conjugates as it has right cosets.

Now in each of the conjugate subgroups of U there are $U:1-1$ elements other than the identity and therefore not in any of the other conjugate subgroups; and there are $G:U$ conjugate subgroups of U. Hence the total number of elements, other than the identity, in the conjugate subgroups of U is
$$(G:U)(U:1-1),$$
i.e.,
$$(G:U)(U:1)-G:U,$$
i.e.,
$$N-G:U$$
i.e.,
$$N-\frac{G:1}{U:1},$$
i.e.,
$$N-\frac{N}{U:1}.$$
We use this to show that G is Abelian.

Suppose that G is not Abelian. Then each element x of G, other than the identity, generates a subgroup (x) which is Abelian and consequently not G; it is therefore a proper subgroup of G. Thus G possesses at least one proper subgroup. Since each proper subgroup of a finite group is contained in at least one maximal proper subgroup, it follows that G possesses at least one maximal proper subgroup. If U is any such, then, since $U:1>1$, the above calculation shows that U and its conjugates supply, in addition to the identity, at least $\frac{1}{2}N$ distinct elements of G. Now if G contained any element y not in U or any of its conjugates, this element would lie in a maximal proper subgroup V of G, and V would contain no element in U or its conjugates other than 1. Hence V and its conjugates would supply at least $\frac{1}{2}N$ distinct elements of G, other than the identity and none of which would be in U or any of its conjugates. Thus U and V and their conjugates would supply more than N distinct elements of G, which is impossible. It follows that U and its conjugates supply all the elements of G, and therefore that
$$1+N-G:U=N;$$

https://doi.org/10.1017/S2040618500035474 Published online by Cambridge University Press

i.e., that $G : U = 1$, i.e., that $U = G$, contrary to the assumption that U was a proper subgroup, Thus the supposition that G is not Abelian leads to a contradiction. We conclude that G must be Abelian.

This completes the proof by induction of the theorem in the case in which the centre of G is the identity.

It follows from the lemma that the multiplicative group K' of the non-zero elements of any finite skew-fields K is Abelian, and therefore that any finite skew-field is a field.

I should like to thank Dr. T. S. Graham for his assistance in preparing for publication this paper and another paper in the present number of these *Proceedings*.

McGill University,
Montreal, Canada.

https://doi.org/10.1017/S2040618500035474 Published online by Cambridge University Press