3. Wedderburn's theorem

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

vectors and they therefore belong to the centre of D since the eigenvectors span D. Each eigenvalue is a root of $f(X)$ so the degree of $g(X)$ is no larger than that of $f(X)$. But $g(\theta) = 0$ so we must have $g(X) = f(X)$. Since each θ_i must be a root of the minimal polynomial of T_θ this proves

(2.4) *The minimal polynomial of* T_θ *is* $f(X)$.

As immediate consequences we have

(2.5) $\dim_F D = \dim_K F =$ degree of $f = m$.

(2.6) $\dim_K D = m^2$.

Finally, we prove

(2.7) *If* $E = K(\theta')$ *and* $f(\theta') = 0$, *then for some non-zero element* d *of* D, $d E d^{-1} \subseteq F$.

To see this, consider the linear transformation $T_{\theta'}$. Since $f(T_{\theta'}) = 0$ there is an eigenvalue $\lambda \in F$ of $T_{\theta'}$ and a corresponding eigenvector d such that $d\theta' = \lambda d$; it follows that $d E d^{-1} \subseteq F$.

Remark. The assumption on the field F amounts to supposing that F/K is a finite Galois extension and the proof of (2.4) shows that $N(F)^{\#}/F^{\#}$ is isomorphic to its Galois group. (Where $F^{\#}$ denotes the set of non-zero elements of F.)

3. Wedderburn's theorem

This proof follows van der Waerden [14, p. 203]. The counting argument was used by Artin [1] in his proof of the same theorem.

THEOREM. *Every finite division ring is a field.*

Proof. Suppose that D is a finite division ring with centre K and maximal subfield F. If the order of F is q, then the elements of F constitute all the roots of the polynomial $X^q - X$; hence any two finite fields of the same order are isomorphic. The multiplicative group of a finite field is cyclic, so $F = K(\theta)$ for some θ. Any element of D is contained in a maximal subfield, which by (2.5) has the same order as F and hence by (2.7) any element of the multiplicative group G of non-zero elements of D belongs to a conjugate of H, the multiplicative group of non-zero elements of F. The number of conjugates of a subgroup is the index of its normalizer, so H has at most $|G : H|$ conjugates in G and hence the union of the conjugates contains at most $|G : H|(|H| - 1) + 1 = |G| - |G : H| + 1$ elements. This number is less than $|G|$ except when $G = H$. Hence $D = F$ is a field.

4. Frobenius' theorem

Let $\mathbf{R}$ denote the field of real numbers, $\mathbf{C}$ the field of complex numbers and $\mathbf{H}$ the division ring of quaternions. The following proof makes use of the fundamental theorem that every polynomial with coefficients in $\mathbf{C}$ has a root in $\mathbf{C}$.

THEOREM. *Let D be a division ring which contains the real numbers* $\mathbf{R}$ *in its centre and suppose that every element of D satisfies a polynomial with coefficients in* $\mathbf{R}$. *Then D is isomorphic to one of* $\mathbf{R}$, $\mathbf{C}$ *or* $\mathbf{H}$.

Proof. Suppose that D is not isomorphic to $\mathbf{R}$ or $\mathbf{C}$. It follows that the maximal subfield F of D is isomorphic to $\mathbf{C}$, the centre K of D is isomorphic to $\mathbf{R}$ and $F = K(i)$ where $i^2 = -1$. Let j be an eigenvector of T_i corresponding to the eigenvalue $-i$. Then $ji = -ij$ and j^2 commutes with j and F. From (2.2) and (2.3) the elements 1 and j form an F-basis for D and therefore $j^2 = \alpha$ belongs to K. If $\alpha = \beta^2$ for some $\beta \in K$ then $(j-\beta)(j+\beta) = 0$ and j belongs to K, which is not the case; hence $\alpha = -\beta^2$ for some $\beta \in K$. Replacing j by $j\beta^{-1}$ we obtain a K-basis $1, i, j, ij$ for D such that $i^2 = j^2 = -1$ and $ij = -ji$. That is, D is isomorphic to $\mathbf{H}$.

An almost identical argument shows that if the dimension of D over its centre K is 4 and the characteristic is not 2, then D has a K-basis $1, i, j, ij$ where $i^2 = \alpha$, $j^2 = \beta$ and $ij = -ji$ for some $\alpha, \beta \in K$.

5. Other proofs of Wedderburn's theorem

The original proofs of the theorem of §3 were given first by Wedderburn [15] in 1905 and then by Dickson [5] in the same year; they depend on certain divisibility properties of the integers. The neatest proof along these lines is that of Witt [16]. Elementary proofs which avoid the use of such number theory have been given by Artin [1] and Herstein [7]. And