2. Division rings

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **25.05.2024**

2. Division rings

By *division ring* we mean an associative ring with identity in which every non-zero element has an inverse. If D is a division ring, the *normalizer* $N(F)$ of a subfield F consists of those elements d such that $dF = Fd$, while the *centralizer* $C(F)$ consists of those elements d such that $dx = xd$ for all x in F; the centralizer is a subdivision ring of D.

From now on D will denote a division ring with centre K and F will denote a maximal subfield of D. We shall assume that $F = K(\theta)$ where θ satisfies an irreducible monic polynomial f with coefficients in K which splits into distinct linear factors over F. We shall see below that this assumption allows us to apply the results of §1 to D considered as a vector space over F (multiplying on the left with elements of F). For each element a of D, the assignment $T_a(d) = da$ defines a linear transformation T_a of this vector space.

If d is an eigenvector of T_θ, then for some λ in F, $d\theta = \lambda d$. This implies that $d\theta d^{-1} = \lambda$ and hence $dFd^{-1} = F$; thus $d \in N(F)$. Conversely, if $d \in N(F)$ and $d \neq 0$, then $d\theta d^{-1} = \lambda \in F$ for some λ and hence d is an eigenvector of T_θ. This proves

(2.1) *A non-zero element d of D is an eigenvector of T_θ if and only if it belongs to $N(F)$.*

Since $f(T_\theta) = 0$, the conditions of §1 apply and we have

(2.2) *The vector space D is the direct sum of the eigenspaces of T_θ.*

Let λ be an eigenvalue of T_θ with eigenvector d, then as above $d\theta = \lambda d$. If d' is another eigenvector, then $d'd^{-1}\lambda d d'^{-1} = \lambda$ and $d'd^{-1}$ centralizes F since $F = K(\lambda)$. However, F is a maximal subfield, and therefore self-centralizing, so $d' = ed$ for some e in F. Thus we obtain

(2.3) *Each eigenspace of T_θ has dimension one.*

Next, we wish to show that $f(X)$ is the minimal polynomial of T_θ. Let $\theta = \theta_1, \theta_2, \ldots, \theta_m$ be the eigenvalues of T_θ and let $1 = d_1, d_2, \ldots, d_m$ be corresponding eigenvectors. Because $N(F)$ is multiplicatively closed $d_i d_j$ must correspond to an eigenvalue θ_k, say, and hence $d_i d_j \theta = \theta_k d_i d_j$, which implies that $d_i \theta_j = \theta_k d_i$. This shows that the mapping which takes θ_j to $d_i \theta_j d_i^{-1}$ permutes the eigenvalues among themselves. Consequently, the coefficients of $g(X) = (X - \theta_1) \ldots (X - \theta_m)$ commute with all the eigenvectors 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