Chapter IX

Simple algebras

§ 1. Structure of simple algebras. This Chapter will be purely algebraic in nature; this means that we will operate over a groundfield, subject to no restriction except commutativity, and carrying no additional structure. All fields are understood to be commutative. All algebras are understood to have a unit, to be of finite dimension over their groundfield, and to be central over that field (an algebra A over K is called central if K is its center). If A, B are algebras over K with these properties, so is $A \otimes_K B$; if A is an algebra over K with these properties, and L is a field containing K, then $A_L = A \otimes_K L$ is an algebra over L with the same properties. Tensor-products will be understood to be taken over the groundfield; thus we write $A \otimes B$ instead of $A \otimes_K B$ when A, B are algebras over K, and $A \otimes L$ or A_L, instead of $A \otimes_K L$, when A is an algebra over K and L a field containing K, A_L being always considered as an algebra over L.

Let A be an algebra over K, with the unit 1_A; all modules over A will be understood to be unitary (this means, e.g. for a left module M, that $1_A \cdot m = m$ for all $m \in M$) and of finite dimension over K, when regarded as vector-spaces over K by putting, e.g. for a left module M, $\xi m = (\xi \cdot 1_A) m$ for all $\xi \in K$ and $m \in M$. If M' is a subset of a left A-module M, the *annihilator* of M' in A is the set of all $x \in A$ such that $xm = 0$ for all $m \in M'$; this is a left ideal in A. The annihilator of M in A is a two-sided ideal in A; if it is $\{0\}$, M is called *faithful*.

Definition 1. *Let A be an algebra over K. An A-module is called simple if it is not $\{0\}$ and has no submodule except itself and $\{0\}$. The algebra A is called simple if it has no two-sided ideal except itself and $\{0\}$.*

For a given A, there are always simple left A-modules; for instance, any left ideal of A, other than $\{0\}$, with the smallest dimension over K, will be such a module.

Proposition 1. *Let A be an algebra over K, with a faithful simple left A-module M. Then every left A-module is a direct sum of modules, all isomorphic to M.*

We first prove our assertion for A itself, considered as a left A-module. In M, there are finite subsets with the annihilator $\{0\}$ in A (e.g. any basis of M over K); take any minimal set $\{m_1, \dots, m_n\}$ with that property. For $0 \leqslant i \leqslant n$, call A_i the annihilator of $\{m_{i+1}, \dots, m_n\}$ in A; for $i \geqslant 1$, put $M_i = A_i m_i$. Clearly $A_0 = \{0\}$, $A_n = A$; for $i \geqslant 1$, $A_i \supset A_{i-1}$, and $A_i \neq A_{i-1}$, since otherwise $xm_j = 0$ for $j > i$ would imply $xm_i = 0$, and m_i could be omitted from $\{m_1, \dots, m_n\}$. For $i \geqslant 1$, A_i is a left ideal, M_i is a submodule of M, and $x \rightarrow xm_i$ induces on A_i a morphism of A_i onto M_i with the kernel A_{i-1}, so that it determines an isomorphism of A_i/A_{i-1} onto M_i for their structures as left A-modules. As $A_i \neq A_{i-1}$, M_i is not $\{0\}$; therefore it is M. By induction on i for $0 \leqslant i \leqslant n$, one sees now at once that $x \rightarrow (xm_1, \dots, xm_i)$ induces on A_i a bijective mapping of A_i onto the product $M^i = M \times \dots \times M$ of i modules, all equal to M; this is obviously an isomorphism for the structure of left A-module. For $i = n$, this proves our assertion for A. Now take any left A-module M', and a finite set $\{m'_1, \dots, m'_r\}$ generating M' (e.g. any basis of M' over K). Then the mapping of A^r into M', given by $(x_i)_{1 \leqslant i \leqslant r} \rightarrow \sum x_i m'_i$, is a surjective morphism of left A-modules; as we have just proved that A, as such, is isomorphic to M^n for some n, this shows that there is a surjective morphism of M^{nr} onto M', or, what amounts to the same, a surjective morphism F, onto M', of a direct sum of $s = nr$ modules M_i, all isomorphic to M. Call N the kernel of F, and take a maximal subset $\{M_{i_1}, \dots, M_{i_h}\}$ of $\{M_1, \dots, M_s\}$ such that the sum $N' = N + \sum M_{i_\lambda}$ is direct; after renumbering the M_i if necessary, we may assume that this subset is $\{M_1, \dots, M_h\}$. Then, for $j > h$, the sum $N' + M_j$ is not direct, so that $N' \cap M_j$ is not $\{0\}$; as it is a submodule of M_j, which is isomorphic to M, it is M_j. This shows that $M_j \subset N'$ for all $j > h$. Therefore F maps N' onto M'; as its kernel is N, it determines an isomorphism of $\sum_{i=1}^{h} M_i$ onto N'.

Proposition 2. *Let A and M be as in proposition 1, and let D be the ring of endomorphisms of M. Then D is a division algebra over K, and A is isomorphic to $M_n(D)$ for some $n \geqslant 1$.*

We recall that here, as explained on p. XV, D should be understood as a ring of right operators on M, the multiplication in it being defined accordingly. As D is a subspace of the ring of endomorphisms of the underlying vector-space of M over K, it is a vector-space of finite dimension over K. Every element of D maps M onto a submodule of M, hence onto M or $\{0\}$; therefore, if it is not 0, it is an automorphism, hence invertible. This shows that D is a division algebra over a center which is of finite dimension over K. By prop. 1, there is, for some $n \geqslant 1$, an isomorphism of A, regarded as a left A-module, onto M^n; this must determine an isomorphism between the rings of endomorphisms of these two left A-modules. Clearly that of M^n consists of the mappings

$$(m_j)_{1 \leqslant j \leqslant n} \to (\sum m_i d_{ij})_{1 \leqslant j \leqslant n}$$

with $d_{ij} \in D$ for $1 \leqslant i,j \leqslant n$, and may therefore be identified with the ring $M_n(D)$ of the matrices (d_{ij}) over D. On the other hand, an endomorphism of A regarded as a left A-module is a mapping f such that $f(xy) = x f(y)$ for all x, y in A; for $y = 1_A$, this shows that f can be written as $x \to xa$ with $a = f(1_A)$; the ring of such endomorphisms may now be identified with A, which is therefore isomorphic to $M_n(D)$. As the center of $M_n(D)$ is clearly isomorphic to that of D, this implies that the latter is K, which completes the proof.

THEOREM 1. *An algebra A over K is simple if and only if it is isomorphic to an algebra $M_n(D)$, where D is a division algebra over K; when A is given, n is uniquely determined, and so is D up to an isomorphism.*

Let A be simple; take any simple left A-module M; as the annihilator of M in A is a two-sided ideal in A and is not A, it is $\{0\}$; therefore M is faithful, and we can apply prop. 2 to A and M; it shows that A is isomorphic to an algebra $M_n(D)$. Conversely, take $A = M_n(D)$. For $1 \leqslant h,k \leqslant n$, call e_{hk} the matrix (x_{ij}) given by $x_{hk} = 1$, $x_{ij} = 0$ for $(i,j) \neq (h,k)$. If $a = (a_{ij})$ is any matrix in $M_n(D)$, we have $e_{ij} a e_{hk} = a_{jh} e_{ik}$ for all i, j, h, k; this shows that, if $a \neq 0$, the two-sided ideal generated by a in A contains all the e_{ik}; therefore it is A, so that A is simple. Let now M be the left ideal generated by e_{11} in A; it consists of the matrices (a_{ij}) such that $a_{ij} = 0$ for $j \geqslant 2$; if a is such a matrix, we have $e_{ij} a = a_{j1} e_{i1}$, which shows that, if $a \neq 0$, the left ideal generated by a is M, which is therefore a minimal left ideal and a simple left A-module. Let now f be an endomorphism of M regarded as a left A-module, and put $f(e_{11}) = a$ with $a = (a_{ij})$, $a_{ij} = 0$ for $j \geqslant 2$. Writing that $f(e_{ij} e_{11}) = e_{ij} a$, we get, for $j \geqslant 2$, $a_{j1} = 0$; then, for $x = (x_{ij})$ with $x_{ij} = 0$ for $j \geqslant 2$, we get $f(x) = f(x e_{11}) = xa = (x_{ij} a_{11})$. This shows that the ring of endomorphisms of M is isomorphic to D. As prop. 1 shows that all simple left A-modules are isomorphic to M, this shows that D is uniquely determined by A up to an isomorphism. As the dimension of A over K is n^2 times that of D, n also is uniquely determined.

We recall now that the *inverse* of an algebra A over K is the algebra A^0 with the same underlying vector-space over K as A, but with the multiplication law changed from $(x,y) \to xy$ to $(x,y) \to yx$.

PROPOSITION 3. *Let A be an algebra over K; call A^0 its inverse, and put $C = A \otimes A^0$. For all a, b in A, call $f(a,b)$ the endomorphism $x \to axb$ of the underlying vector-space of A; let F be the K-linear mapping of C into $\mathrm{End}_K(A)$ such that $F(a \otimes b) = f(a,b)$ for all a, b. Then A is simple if and only if F maps C surjectively onto $\mathrm{End}_K(A)$; when that is so, F is an isomorphism of C onto $\mathrm{End}_K(A)$.*

One verifies at once that F is a homomorphism of C into $\mathrm{End}_K(A)$. If N is the dimension of A over K, both C and $\mathrm{End}_K(A)$ have the dimension N^2 over K; therefore F is an isomorphism of C onto $\mathrm{End}_K(A)$ if and only if it is surjective, and if and only if it is injective. Assume that A is not simple, i.e. that it has a two-sided ideal I other than $\{0\}$ and A. Then, for all $a, b, f(a,b)$ maps I into I; therefore the same is true of $F(c)$ for all $c \in C$, so that the image of C under F is not the whole of $\mathrm{End}_K(A)$. Assume now that A is simple, and call M the underlying vector-space of A over K, regarded as a left C-module for the law $(c,x) \to F(c)x$. Any submodule M' of M is then mapped into itself by $x \to axb$ for all a, b, so that it is a two-sided ideal in A; as A is simple, this shows that M is simple. An endomorphism φ of M is a mapping φ such that $\varphi(axb) = a\varphi(x)b$ for all a, x, b in A; for $x = b = 1_A$, this gives $\varphi(a) = a\varphi(1_A)$, hence $axb\varphi(1_A) = ax\varphi(1_A)b$, so that $\varphi(1_A)$ must be in the center K of A; in other words, φ is of the form $x \to \xi x$ with $\xi \in K$. Call C' the annihilator of M in C, which is the same as the kernel of F. We can now apply prop. 2 to the algebra C/C', to its center Z, and to the module M; as D is then K, it shows that C/C' is isomorphic to some $M_n(K)$, hence Z to K; but then, as has been seen in the proof of th. 1, M must have the dimension n over K, so that $n = N$. As C/C' has then the same dimension N^2 over K as C, we get $C' = \{0\}$, which completes the proof. *

COROLLARY 1. *Let L be a field containing K. Then the algebra $A_L = A \otimes L$ over L is simple if and only if A is so.*

In fact, let C_L, F_L be defined for A_L just as C, F are defined for A in proposition 3; one sees at once that $C_L = C \otimes L$, and that F_L is the L-linear extension of F to C_L. Our assertion follows now from proposition 3.

COROLLARY 2. *Let L be an algebraically closed field containing K. Then A is simple if and only if A_L is isomorphic to some $M_n(L)$.*

If D is a division algebra over a field K, the extension of K generated in D by any $\xi \in D - K$ is an algebraic extension of K, other than K. In particular, if L is algebraically closed, there is no division algebra over L, other than L. Therefore, by th. 1, an algebra over L is simple if and only if it is isomorphic to some $M_n(L)$. Our assertion follows now from corollary 1.

COROLLARY 3. *The dimension of a simple algebra A over K is of the form n^2.*

In fact, by corollary 2, A_L is isomorphic to some $M_n(L)$ if L is an algebraic closure of K; its dimension over L is then n^2, and it is the same as that of A over K.

COROLLARY 4. *Let A, B be two simple algebras over K; then $A\otimes B$ is simple over K.*

Take an algebraic closure L of K; $(A\otimes B)_L$ is the same as $A_L\otimes B_L$. Since clearly $M_n(K)\otimes M_m(K)$ is isomorphic to $M_{nm}(K)$ for all m, n, and all fields K, our conclusion follows from corollary 2.

COROLLARY 5. *Let A be a simple algebra of dimension n^2 over K. Let L be a field containing K, and let F be a K-linear homomorphism of A into $M_n(L)$. Then the L-linear extension F_L of F to A_L is an isomorphism of A_L onto $M_n(L)$.*

Clearly F_L is a homomorphism of A_L into $M_n(L)$, so that its kernel is a two-sided ideal in A_L. As A_L is simple by corollary 1, and as F_L is not 0, this kernel is $\{0\}$, i.e. F_L is injective. As A_L and $M_n(L)$ have the same dimension n^2 over L, this implies that it is bijective, so that it is an isomorphism of A_L onto $M_n(L)$.

COROLLARY 6. *Let L be an extension of K of degree n; let A be a simple algebra of dimension n^2 over K, containing a subfield isomorphic to L. Then A_L is isomorphic to $M_n(L)$.*

We may assume that A contains L. Then $(x,\xi)\to x\xi$, for $x\in A$, $\xi\in L$, defines on A a structure of vector-space over L; call V that vector-space, which is clearly of dimension n over L. For every $a\in A$, the mapping $x\to ax$ may be regarded as an endomorphism of V, which, if we choose a basis for V over L, is given by a matrix $F(a)$ in $M_n(L)$. Our assertion follows now from corollary 5.

PROPOSITION 4. *Let A be a simple algebra over K. Then every automorphism α of A over K is of the form $x\to a^{-1}xa$ with $a\in A^\times$.*

Take a basis $\{a_1,\dots,a_N\}$ of A over K. Then every element of $A\otimes A^0$ can be written in one and only one way as $\sum a_i\otimes b_i$, with $b_i\in A^0$ for $1\leqslant i\leqslant N$. By prop. 3, α can therefore be written as $x\to\sum a_i x b_i$. Writing that $\alpha(xy)=\alpha(x)\alpha(y)$ for all x, y, we get

$$0=\sum a_i x y b_i-\sum a_i x b_i\alpha(y)=\sum a_i x(yb_i-b_i\alpha(y)).$$

For each $y\in A$, this is so for all x; by prop. 3, we must therefore have $yb_i=b_i\alpha(y)$. In particular, since this gives $y(b_i z)=b_i\alpha(y)z$ for all y and z in A, b_iA is a two-sided ideal in A, hence A or $\{0\}$, for all i, so that b_i is either 0 or invertible in A. As α is an automorphism, the b_i cannot all be 0; taking $a=b_i\neq 0$, we get the announced result.

COROLLARY. *Let α and a be as in proposition 4, and let $a'\in A$ be such that $a'\alpha(x)=xa'$ for all $x\in A$. Then $a'=\xi a$ with $\xi\in K$.*

In fact, the assumption can be written as $a'a^{-1}x=xa'a^{-1}$ for all x; this means that $a'a^{-1}$ is in the center K of A.

Proposition 4 is generally known as "the theorem of Skolem-Noether" (although that name is sometimes reserved for a more complete statement involving a simple subalgebra of A). One can prove, quite similarly, that every derivation of A is of the form $x\to xa-ax$, with $a\in A$.

We will also need a stronger result than corollary 2 of prop. 3; this will appear as a corollary of the following:

PROPOSITION 5. *Let D be a division algebra over K, other than K. Then D contains a separably algebraic extension of K, other than K.*

We reproduce Artin's proof. In D, considered as a vector-space over K, take a supplementary subspace E to $K=K\cdot 1_D$, and call φ the projection from $D=E\oplus K\cdot 1_D$ onto E. Then, for every integer $m\geqslant 1$, $x\to\varphi(x^m)$ is a polynomial mapping of D into E, whose extension to D_L and E_L, if L is any field containing K, is again given by $x\to\varphi(x^m)$, where φ denotes again the L-linear extension of φ to D_L and E_L. Now call N the dimension of D over K. Clearly every $\xi\in D$, not in K, generates over K an extension $K(\xi)$ of degree >1 and $\leqslant N$; moreover, if this is not purely inseparable over K, it contains a separable extension of K, other than K. Assume now that our proposition is not true for D. Then K has inseparable extensions, which implies that it is of characteristic $p>1$ and that it is not a finite field; moreover, every $\xi\in D$ must be purely inseparable over K, hence must satisfy an equation $\xi^{p^n}=x\in K$, where p^n is its degree over K. As this degree is $\leqslant N$, it divides the highest power q of p which is $\leqslant N$, so that $\xi^q\in K$. Then, if E and φ are as above defined, the polynomial mapping $x\to\varphi(x^q)$ maps D onto 0. As K is an infinite field, this implies that the same holds true for the extension of that mapping to D_L and E_L, when L is any field containing K. In other words, for all L, $x\to x^q$ maps D_L into its center $L\cdot 1_D$. This is palpably false when L is algebraically closed, for then D_L is isomorphic to an algebra $M_n(L)$, and taking e.g. $x=e_{11}$ in the notation of the proof of th. 1, we have $x^q=e_{11}$, and this is not in the center of $M_n(L)$.

COROLLARY. *Let A be a simple algebra over K, and L a separably algebraically closed field containing K. Then A_L is isomorphic to an algebra $M_n(L)$.*

The assumption means that L has no separably algebraic extension other than itself. Then proposition 5 shows that there is no division algebra over L, other than L. Our conclusion follows now at once from th. 1, combined with corollary 1 of prop. 3.

§ 2. The representations of a simple algebra. Let A be a simple algebra over K; by corollary 3 of prop. 3, § 1, its dimension N over K may be written as $N=n^2$. For any field L containing K, call $\mathfrak{M}_L$ the space of the K-linear mappings of A into $M_n(L)$; every such mapping F can be uniquely extended to an L-linear mapping F_L of A_L into $M_n(L)$. If one takes a basis $\alpha=\{a_1,\dots,a_N\}$ of A over K, F is uniquely determined by the N matrices $X_i=F(a_i)$, so that, by the choice of this basis, $\mathfrak{M}_L$ is identified with the space of the sets $(X_i)_{1\leqslant i\leqslant N}$ of N matrices in $M_n(L)$, which is obviously of dimension N^2 over L.

By corollary 5 of prop. 3, § 1, a mapping $F\in\mathfrak{M}_L$ is an isomorphism of A into $M_n(L)$, and its extension F_L to A_L is an isomorphism of A_L onto $M_n(L)$, if and only if F is a homomorphism, i.e. if and only if $F(1_A)=1_n$ and $F(ab)=F(a)F(b)$ for all a, b in A, or, what amounts to the same, for all a, b in the basis α. When that is so, we say that F is an *L-representation* of A; if we write $K(F)$ for the field generated over K by the coefficients of the matrices $F(a)$ for all $a\in A$, or, what amounts to the same, for all $a\in\alpha$, then F is also a $K(F)$-representation of A.

If L is suitably chosen (for instance, by corollary 2 of prop. 3, § 1, if it is algebraically closed, or even, by the corollary of prop. 5, § 1, if it is separably algebraically closed), the set of L-representations of A is not empty. Moreover, if F and F' are in that set, then $F'_L\circ F_L^{-1}$ is an automorphism of $M_n(L)$, hence, by prop. 4 of § 1, of the form $X\to Y^{-1}XY$ with $Y\in M_n(L)^\times$; this can be written as $F'_L(F_L^{-1}(X))=Y^{-1}XY$; for $a\in A$, $X=F(a)$, it implies $F'(a)=Y^{-1}F(a)Y$; we express this by writing $F'=Y^{-1}FY$. Moreover, when F and F' are given, the corollary of prop. 4, § 1, shows that Y is uniquely determined up to a factor in the center $L^\times$ of $M_n(L)^\times$.

Proposition 6. *Let A be a simple algebra of dimension n^2 over K. Then there is a K-linear form $\tau\neq 0$ and a K-valued function ν on A, such that, if L is any field containing K, and F any L-representation of A, $\tau(a)=\mathrm{tr}(F(a))$ and $\nu(a)=\det(F(a))$ for all $a\in A$; if K is an infinite field, ν is a polynomial function of degree n on A.*

Put $N=n^2$, and take a basis $\{a_1,\dots,a_N\}$ of A over K. Take first for L a "separable algebraic closure" of K, i.e. the union of all separably algebraic extensions of K in some algebraically closed field containing K; this is always an infinite field. By the corollary of prop. 5, § 1, there is an L-representation F of A, and then, as we have seen above, all such representations can be written as $F'=Y^{-1}FY$ with $Y\in M_n(L)^\times$. Clearly $a\to\mathrm{tr}(F_L(a))$ is an L-linear form τ on A_L, and $a\to\det(F_L(a))$ is a polynomial function ν of degree n on A_L; as F_L is an isomorphism of A_L onto $M_n(L)$, τ is not 0; neither τ nor ν is changed if F is replaced by $F'=Y^{-1}FY$. Writing $a=\sum x_i a_i$ with $x_i\in L$ for $1\leqslant i\leqslant N$, we can write τ and ν as a linear form and as a homogeneous polynomial of degree n, respectively, in the x_i, with coefficients in L. If σ is any automorphism of L over K, we will write τ^σ, ν^σ for the polynomials in the x_i, respectively derived from τ, ν by substituting for each coefficient its image under σ. Similarly, we write F^σ for the L-representation of A such that, for each a in the basis $\{a_1,\dots,a_N\}$, $F^\sigma(a)$ is the image $F(a)^\sigma$ of $F(a)$ under σ, i.e. the matrix whose coefficients are respectively the images of those of $F(a)$. Then, clearly, for all $a\in A_L$, $\tau^\sigma(a)$ and $\nu^\sigma(a)$ are respectively the trace and the determinant of $F^\sigma(a)$; as we have seen above, they must therefore be equal to $\tau(a)$, $\nu(a)$ for all $a\in A_L$. This implies that all the coefficients in τ and ν, when these are written as polynomials in the x_i, are invariant under all automorphisms of L over K, hence that they are in K. This proves our assertion, so far as only L-representations are concerned, with L chosen as above. Obviously it remains true for L'-representations if L' is any field containing L. As every field containing K is isomorphic over K to a subfield of such a field L', this completes the proof.

The functions τ, ν defined in proposition 6 are called *the reduced trace* and *the reduced norm* in A. Clearly $\tau(xy)=\tau(yx)$ and $\nu(xy)=\nu(x)\nu(y)$ for all x, y in A; in particular, ν determines a morphism of $A^\times$ into $K^\times$.

Corollary 1. *Let A and ν be as in proposition 6. Then, for every $a\in A$, the endomorphisms $x\to ax$, $x\to xa$ of the underlying vector-space of A over K have both the determinant $N_{A/K}(a)=\nu(a)^n$.*

It is clearly enough to verify this for A_L with a suitable L; taking L such that A_L is isomorphic to $M_n(L)$, we see that it is enough to verify it for an algebra $M_n(L)$ over L; but then it is obvious. This is the result announced in the remarks preceding th. 4 of Chap. IV-3.

Corollary 2. *Let D be a division algebra over K; let τ_0, ν_0 be the reduced trace and the reduced norm in D. For any $m\geqslant 1$, put $A=M_m(D)$, and call τ, ν the reduced trace and the reduced norm in A. Then, for every $x=(x_{ij})$ in A, $\tau(x)=\sum_i\tau_0(x_{ii})$; if the matrix $x=(x_{ij})$ in A is triangular, i.e. if $x_{ij}=0$ for $1\leqslant j<i\leqslant m$, $\nu(x)=\prod_i\nu_0(x_{ii})$.*

Take L such that D has an L-representation F. Then the mapping which, to every matrix $x=(x_{ij})$ in $M_m(D)$, assigns the matrix obtained by substituting the matrix $F(x_{ij})$ for each coefficient x_{ij} in x is an L-representation of A. Using this for defining τ and ν, we get at once the conclusion of our corollary.

Corollary 3. *Let assumptions and notations be as in corollary 2. Then* $\nu(A^\times)=\nu_0(D^\times)$.

We may regard A as the ring of endomorphisms of the space $V=D^m$ considered as a left vector-space over D, and consequently $A^\times$ as the group of automorphisms of that space. By an elementary result (already used in the proof of corollary 3 of th. 3, Chap. I-2, but only for a vector-space over a commutative field), every automorphism of V can be written as a product of automorphisms, each of which is either a permutation of the coordinates or of the form

$$(x_1,\dots,x_m)\to(\sum_i x_i a_i, x_2,\dots,x_m)$$

with $a_1\in D^\times$ and $a_i\in D$ for $2\leqslant i\leqslant m$. By corollary 2, the latter automorphism has the reduced norm $\nu_0(a_1)$. As to a permutation of coordinates, the same L-representation of A which was used in the proof of corollary 2 shows at once that it has the reduced norm 1 if the dimension d^2 of D over K is even, and ± 1 if it is odd. As $\nu_0(-1_D)=(-1)^d$, we have thus shown that $\nu(A^\times)$ contains $\nu_0(D^\times)$ and is contained in it.

§ 3. Factor-sets and the Brauer group. Up to an isomorphism, the algebras over a given field K may be regarded as making up a set, since the algebra structures that one can put on a given vector-space over K clearly make up a set, and every such space is isomorphic to K^n for some n.

From now on, we will consider only *simple* algebras over K; it is still understood that they are of finite dimension and central over K. Consider two such algebras A, A'; by th. 1 of § 1, they are isomorphic to algebras $M_n(D)$, $M_{n'}(D')$, where D, D' are division algebras over K which are uniquely determined, up to an isomorphism, by A, A'. One says then that A and A' are *similar*, and that they belong to the same *class*, if D and D' are isomorphic over K. Clearly, in each class of simple algebras, there is, up to an isomorphism, one and only one division algebra, and there is at most one algebra of given dimension over K. An algebra will be called *trivial* over K if it is similar to K, i.e. isomorphic to $M_n(K)$ for some n. We will write $\mathrm{Cl}(A)$ for the class of simple algebras similar to a given one A.

Let A, A' be two simple algebras, respectively isomorphic to $M_n(D)$ and to $M_{n'}(D')$, where D, D' are division algebras over K. By corollary 4 of prop. 3, § 1, $D\otimes D'$ is simple, hence isomorphic to an algebra $M_m(D'')$, where D'' is a division algebra over K which is uniquely determined, up to an isomorphism, by D and D', hence also by A and A'. By the associativity of tensor-products, $A\otimes A'$ is isomorphic to $M_{nn'm}(D'')$. This shows that the class of $A\otimes A'$ is uniquely determined by those of A and A'. Write now:

$$\mathrm{Cl}(A\otimes A')=\mathrm{Cl}(A)\cdot\mathrm{Cl}(A'),$$

and consider this as a law of composition in the set of classes of simple algebras over K. It is clearly associative and commutative; it has a neutral element, viz., the class $\mathrm{Cl}(K)$ of trivial algebras over K. Moreover, if A^0 is the inverse algebra to A, prop. 3 of § 1 shows that $A\otimes A^0$ is trivial, so that $\mathrm{Cl}(A^0)$ is the inverse of $\mathrm{Cl}(A)$ for our law of composition. Therefore, for this law, the classes of simple algebras over K make up a group; this is known as *the Brauer group of* K; we will denote it by $B(K)$. If K' is any field containing K, and A a simple algebra over K, it is obvious that the class of $A_{K'}$ is determined uniquely by that of A, and that the mapping $\mathrm{Cl}(A)\to\mathrm{Cl}(A_{K'})$ is a morphism of $B(K)$ into $B(K')$, which will be called *the natural morphism* of $B(K)$ into $B(K')$.

It will now be shown that the Brauer group can be defined in another way, by means of "factor-sets"; this will require some preliminary definitions. We choose once for all an algebraic closure $\bar{K}$ for K; we will denote by K_{sep} the maximal separable extension of K in $\bar{K}$, i.e. the union of all separable extensions of K of finite degree, contained in $\bar{K}$. We will denote by $\mathfrak{G}$ the Galois group of K_{sep} over K, topologized as usual by taking, as a fundamental system of neighborhoods of the identity ε, all the subgroups of $\mathfrak{G}$ attached to separable extensions of K of finite degree. Clearly this makes $\mathfrak{G}$ into a totally disconnected compact group. As $\bar{K}$ is purely inseparable over K_{sep}, each automorphism of K_{sep} can be uniquely extended to one of $\bar{K}$, so that $\mathfrak{G}$ may be identified with the group of all automorphisms of $\bar{K}$ over K.

Definition 2. *Let* $\mathfrak{G}^{(m)}$ *be the product* $\mathfrak{G}\times\cdots\times\mathfrak{G}$ *of m factors equal to* $\mathfrak{G}$; *let* $\mathfrak{H}$ *be an open subgroup of* $\mathfrak{G}$. *Then a mapping f of* $\mathfrak{G}^{(m)}$ *into any set S will be called* $\mathfrak{H}$*-regular if it is constant on left cosets in* $\mathfrak{G}^{(m)}$ *with respect to* $\mathfrak{H}^{(m)}$.

This amounts to saying that $f(\sigma_1,\dots,\sigma_m)$ depends only upon the left cosets $\mathfrak{H}\sigma_1,\dots,\mathfrak{H}\sigma_m$ determined by the σ_i in $\mathfrak{G}$. When that is so, f is locally constant, or, what amounts to the same, it is continuous when S is provided with the discrete topology. Conversely, let f be a mapping of $\mathfrak{G}^{(m)}$ into S; if it is locally constant, it is continuous if S is topologized discretely, hence uniformly continuous since $\mathfrak{G}$ is compact; this implies that there is an open subgroup $\mathfrak{H}$ of $\mathfrak{G}$ such that f is $\mathfrak{H}$-regular.