CHAPTER 1

Background material

1.1 Rings and modules

Good references for this section are [31], [11] and [10]. We assume known the rudiments of the theory of rings and modules, such as direct sums, factor rings and modules, exact sequences, algebras over a field, tensor products of modules over (possibly noncommutative) rings, tensor products of algebras, etc. Most statements will be made for left modules only, with the understanding that with the obvious changes, they apply to right modules as well.

We also assume the language and basic facts about categories and functors.

Let R be a ring. A left R-module M is sometimes denoted by ${}_RM$, a right R-module by M_R, and an (R, S)-bimodule by ${}_RM_S$.

A *simple*[1] R-module M is a nonzero module whose only submodules are 0 and M. It follows that a homomorphism between two simple modules must be either an isomorphism or 0, so the endomorphism ring $\mathrm{End}_R M$ of a simple module is a division ring ("Schur's Lemma ").

A Jordan-Hölder series for M is a series of submodules

$$\{0\} = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M,$$

in which each factor M_i/M_{i-1} is a simple module. If M *has* a Jordan-Hölder series, M is said to be of *finite length*, and its *length*, $\mathrm{len}_R M = n$, is well-defined. If

$$0 \to N \to M \to Q \to 0$$

is an exact sequence of R-modules, M has finite length if and only if both N and Q do, and then

$$\mathrm{len}_R M = \mathrm{len}_R N + \mathrm{len}_R Q.$$

The ring of $n \times n$ matrices over R is denoted by $\mathrm{M}(n, R)$, and $\mathbf{GL}(n, R)$ is the "general linear group" of invertible matrices in $\mathrm{M}(n, R)$. The R-module – actually (R, R)-bimodule – of $n \times m$ matrices is $R^{n\times m}$; it is also an $(\mathrm{M}(n, R), \mathrm{M}(m, R))$-bimodule.

Let M be a right R-module and N a left R-module. A map $\varphi : M \times N \to P$ into an Abelian group P is *balanced* (*over* R) if it satisfies $\varphi(ur, v) = \varphi(u, rv)$ for all $u \in M, v \in N$, and $r \in R$. We sometimes also say that φ *admits* R. It is *biadditive* if it is additive in each variable.

The tensor product $M \otimes_R N$ is an Abelian group together with a balanced biadditive map can : $M \times N \to M \otimes_R N$ over R, with the following universal mapping property: *if* $\varphi : M \times N \to P$ *is a balanced biadditive map over* R *into an*

[1] sometimes called *irreducible*, as in [31].

Abelian group P, there is a unique homomorphism $\hat{\varphi} : M \otimes_R N \to P$ of Abelian groups which makes the diagram

$$\begin{tikzcd} M \times N \arrow[r, "\mathrm{can}"] \arrow[dr, "\varphi"'] & M \otimes_R N \arrow[d, "\hat{\varphi}"] \\ & P \end{tikzcd}$$

commutative. The image of (u, v) in $M \otimes_R N$ under the canonical map is denoted by $u \otimes_R v$ or simply $u \otimes v$.

If M is an (S, R)-bimodule, $M \otimes_R N$ is (in a natural way) a left S-module. Similarly it is a right T-module if N is an (R, T)-bimodule, and if P is a left T-module, there is a canonical isomorphism

$$(M \otimes_R N) \otimes_T P \cong M \otimes_R (N \otimes_T P).$$

And if M and N are both bimodules as above, then $M \otimes_R N$ is an (S, T)-bimodule.

There are also canonical isomorphisms

$$R \otimes_R M \cong M, \quad (\oplus_i M_i) \otimes_R N \cong \oplus_i (M_i \otimes_R N), \quad M \otimes_R (\oplus_i N_i) \cong \oplus_i (M \otimes_R N_i).$$

If M and N are (say) left R-modules, similar remarks apply to the Abelian group $\mathrm{Hom}_R(M, N)$. For example if M is an (R, S)-bimodule, then $\mathrm{Hom}_R(M, N)$ is a left S-module, while if N is an (R, T)-bimodule, $\mathrm{Hom}_R(M, N)$ is a right T-module, via

$$(s\varphi)(u) = \varphi(us) \text{ and } (\varphi t)(u) = \varphi(u)t.$$

We will generally write homomorphisms on the left, although in certain circumstances it is better to write them on the right (opposite to the scalars) and we will do so.

For finite direct sums, there are canonical isomorphisms

$$\begin{aligned} \mathrm{Hom}_R(\oplus_i M_i, N) &\cong \oplus_i \mathrm{Hom}_R(M_i, N) \\ \mathrm{Hom}_R(M, \oplus_i N_i) &\cong \oplus_i \mathrm{Hom}_R(M, N_i). \end{aligned} \tag{1.1}$$

Now write homomorphisms on the right, and consider the (internal) direct sum $M = M_1 \oplus \cdots \oplus M_m$ of left R-modules, and let

$$\iota_i = \iota_i^M : M_i \to M, \quad \pi_i = \pi_i^M : M \to M_i \tag{1.2}$$

be the associated injections and projections (written on the *right*). They satisfy

$$\iota_j \pi_i = 0 \text{ if } i \neq j, \quad \iota_i \pi_i = \mathrm{id}_{M_i}, \quad \text{and} \quad \sum_i \pi_i \iota_i = \mathrm{id}_M. \tag{1.3}$$

These conditions characterize the direct sum; that is to say if $M_1, \ldots, M_m$ are R-modules and homomorphisms (1.2) satisfying (1.3) are given, then M is the internal direct sum of its submodules $M_i \iota_i$ – or alternatively the map $\oplus_i \pi_i : M \to M_1 \oplus \cdots \oplus M_m$ is an isomorphism of M with the external direct sum.

If $N = N_1 \oplus \cdots \oplus N_n$ and $\varphi : M \to N$ is a homomorphism, define

$$\varphi_{ij} = \iota_i^M \varphi \pi_j^N : M_i \to N_j.$$

The matrix (φ_{ij}) describes φ completely since $\sum_{i,j} \pi_i \varphi_{ij} \iota_j = \varphi$. Conversely any matrix (φ_{ij}) of homomorphisms $\varphi_{ij} : M_i \to N_j$ corresponds uniquely to a homomorphism $\varphi : M \to N$ with the components φ_{ij}. Furthermore if $\psi : N \to P =$

$P_1 \oplus \cdots \oplus P_p$ is a second homomorphism, the matrix of $\varphi\psi$ is the matrix product $(\varphi_{ij})(\psi_{kl})$. Thus if M^m denotes the m-fold direct sum of M with itself and homomorphisms are written on the right,

Proposition 1.1.1 *(a)* $(\mathrm{End}_R M)^{m\times k}$ *is isomorphic to* $\mathrm{Hom}_R(M^m, M^k)$*, via "multiplication"*

$$(u_1, u_2, \ldots, u_m)(\varphi_{ij}) = \left(\sum_i u_i\varphi_{i1}, \ldots, \sum_i u_i\varphi_{ik}\right).$$

(b) The ring of endomorphisms $\mathrm{End}_R(M^m)$ *(operating on the* right *of* M^m*) is isomorphic to the matrix ring* $\mathrm{M}(m, \mathrm{End}_R M)$*. In particular if M is simple, then* $\mathrm{End}_R(M^m)$ *is isomorphic to the matrix ring* $\mathrm{M}(m, D)$ *where D is the division ring* $\mathrm{End}_R M$*.*

(c) The isomorphism

$$(\mathrm{End}_R M)^{m\times k} \to \mathrm{Hom}_R(M^m, M^k)$$

in (a) is an $(\mathrm{End}_R(M^m), \mathrm{End}_R(M^k))$*-bimodule isomorphism.*

(a) and (b) have already been proved. In (c), it is understood that $\mathrm{End}_R(M^m)$ operates on $(\mathrm{End}_R M)^{m\times k}$ through the isomorphism $\mathrm{End}_R(M^m) \to \mathrm{M}(m, \mathrm{End}_R M)$ of (b) and left multiplication, and that $\mathrm{End}_R(M^k)$ operates on $(\mathrm{End}_R M)^{m\times k}$ through the isomorphism $\mathrm{End}_R(M^k) \to \mathrm{M}(k, \mathrm{End}_R M)$ and right multiplication. (c) follows directly from this and the fact that, in general, $\mathrm{Hom}_R({}_RM_S, {}_RN_T)$ is an (S,T)-bimodule via $(s\varphi t)(u) = \varphi(us)t$. □

An *R-pairing* is an R-bilinear map

$$U \times W \to R, \quad (u, w) \to \langle u, w\rangle, \tag{1.4}$$

involving a left R-module U and a right R-module W. This means the map is biadditive and satisfies

$$\langle au, wb\rangle = a\langle u, w\rangle b \text{ for all } u \in U,\ w \in W \text{ and } a, b \in R.$$

The *R-dual* of a left R-module M is the right R-module $M^* = \mathrm{Hom}_R(M, R)$ where R is considered as a left R-module via multiplication. The module structure of M^* is determined by

$$(xr)(u) = (xu)r \quad (x \in M^*, r \in R, u \in M), \tag{1.5}$$

now writing homomorphisms on the left. We also use the pairing notation:

$$M \times M^* \to R, \quad (u, x) \to \langle u, x\rangle = x(u). \tag{1.6}$$

Then (1.5) becomes

$$\langle u, xr\rangle = \langle u, x\rangle r.$$

If M is an (R,S)-bimodule, then M^* is an (S,R)-bimodule via

$$\langle u, sxr\rangle = \langle us, x\rangle r.$$

Suppose that $M = N \oplus P$. If $N^o = \{x \in M^* |\ \langle N, x\rangle = 0\}$ is the annihilator of N and P^o that of P, then $M^* = P^o \oplus N^o$ (internal direct sum), $P^o \cong N^*$ and $N^o \cong P^*$ via the restriction maps $M^* \to N^*$, $x \to x|_N$, and $M^* \to P^*$, $x \to x|_P$. If we identify via these isomorphisms,

$$M^* = N^* \oplus P^*.$$

By induction if $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$, then

$$M^* = M_1^* \oplus M_2^* \oplus \cdots \oplus M_n^*, \tag{1.7}$$

where M_i^* is the annihilator of $\oplus_{j \neq i} M_j$, and is the dual of M_i when the pairing (1.6) is restricted to $M_i \times M_i^*$.

If $\varphi : M \to N$ is an R-homomorphism, then $\varphi^t : N^* \to M^*$ is the *transpose* of φ, the R-homomorphism determined by

$$\langle u, \varphi^t x \rangle = \langle \varphi u, x \rangle. \tag{1.8}$$

If $\psi : N \to P$ is another R-homomorphism, then

$$(\psi\varphi)^t = \varphi^t \psi^t.$$

It follows that φ^t is an isomorphism if φ is.

Definition 1.1.1 *An* involution *on the ring R is an automorphism $r \to \bar{r}$ of R as an additive group such that*
1. $\bar{\bar{r}} = r$,
2. $\overline{r_1 r_2} = \overline{r_2}\,\overline{r_1}$ *for all* $r, r_1, r_2 \in R$.

The pair $(R, {}^-)$ *is called a* ring with involution, *or an* involution ring.

If R is a field K, then of course $(K, {}^-)$ is called a field with involution, *or an involution field.*

If $(K, {}^-)$ is a field with involution, a $(K, {}^-)$-involution algebra, or an algebra with $(K, {}^-)$-involution, is a pair $(A, {}^-)$ where A is a K-algebra with an involution ${}^-$ which is compatible with that on K:
3. $\overline{\alpha a} = \bar{\alpha}\bar{a}$ *for all* $\alpha \in K$ *and* $a \in A$.

Briefly, an involution of a ring R is an antiautomorphism of R of period 1 or 2; when the period is 1 (i.e. the involution is the identity map id_R), then R must be commutative.

It is occasionally necessary to consider, a little more generally, an involution algebra $(A, {}^-)$ over a commutative ring $(C, {}^-)$ with involution, defined in the obvious way.

A *homomorphism* $\varphi : (R, {}^-) \to (S, {}^-)$ of rings with involution is a ring homomorphism $R \to S$ which commutes with the involutions: $\varphi(\bar{r}) = \overline{\varphi(r)}$ for all $r \in R$. And a homomorphism of involution algebras is one of rings with involution which commutes with the scalars. Thus an isomorphism of rings or algebras with involution is such a map which is an isomorphism of rings or algebras; we then also say that the involutions on R and S are *equivalent*.

A right R-module M can be "twisted" into a left R-module in the presence of an involution on R. Namely we define $ru = u\bar{r}$. It is often convenient to denote the twisted R-module M by $\bar{M}$ and its elements by $\bar{u}$. Thus $\bar{u} = u$ but $\bar{u}$ is considered to be a member of $\bar{M}$. This leads to the appealing equation $\overline{ur} = \bar{r}\bar{u}$, but we use it more often in the form $r\bar{u} = \overline{u\bar{r}}$. Similarly if M is an (R, S)-bimodule and R and S both have involutions, M can be twisted into an (S, R)-bimodule $\bar{M}$ via $s\bar{u}r = \overline{\bar{r}u\bar{s}}$.

Theorem 1.1.1 *Let V be a vector space over the field K spanned by the vectors $v_1, v_2, \dots, v_n$ over K. Suppose further that there is a bilinear multiplication $V \times V \to V$ which is associative on the generators $v_1, v_2, \dots, v_n$. Then V, with this multiplication, is an "algebra without 1" over K.* □

Theorem 1.1.2 *Suppose that A is an algebra over the field K, M is a right A-module and N a left A-module. If L/K is a field extension, there is a canonical isomorphism (of L-vector spaces)*

$$L \otimes_K (M \otimes_A N) \xrightarrow{\sim} (L \otimes_K M) \otimes_{L \otimes_K A} (L \otimes_K N),$$

given by

$$\lambda \otimes (u \otimes v) \to (\lambda \otimes u) \otimes (1 \otimes v).$$

It is understood that M is a right K-vector space through the action of A, and so also a left K-vector space since K is commutative: $\alpha u = u\alpha \ \ (u \in M, \alpha \in K)$. Also $L \otimes_K M$, for example, is a right $L \otimes_K A$-module via the action $(\lambda \otimes u)(\mu \otimes a) = \lambda\mu \otimes ua$. And we assume that A is imbedded in $L \otimes_K A$ via $a \to 1 \otimes a$.

First of all, the map $M \times N \to (L \otimes_K M) \otimes_{L \otimes_K A} (L \otimes_K N)$, $(x, y) \to (1 \otimes M) \otimes (1 \otimes y)$, is balanced over A, and so we get a homomorphism $M \otimes_A N \to (L \otimes_K M) \otimes_{L \otimes_K A} (L \otimes_K N)$. Then the map $L \times (M \otimes_A N) \to (L \otimes_K M) \otimes_{L \otimes_K A} (L \otimes_K N)$ is balanced over K and so we get the map φ of the theorem.

On the other hand, the map $(\sum_i \lambda_i \otimes u_i, \sum_j \mu_j \otimes v_j) \to \sum_{i,j} (\lambda_i \mu_j) \otimes (u_i \otimes v_j)$ is a biadditive map $(L \otimes_K M) \times (L \otimes_K N) \to L \otimes_K (M \otimes_A N)$, balanced over $L \otimes_K A$; the only problem is to show that it is well-defined. Once we have done this, we will have a homomorphism $\psi : (L \otimes_K M) \otimes_{L \otimes_K A} (L \otimes_K N) \to L \otimes_K (M \otimes_A N)$ which is inverse to φ, and so both are isomorphisms. It is clear that they are L-isomorphisms, and so the theorem will have been proved.

Suppose then that $\lambda, \mu \in L$, $u \in M$, and $v \in N$. The map $(\lambda, u) \to \lambda\mu \otimes_K (u \otimes_A v)$ is biadditive and balanced over K, so gives a homomorphism $L \otimes_K M \to L \otimes_K (M \otimes_A N)$ of Abelian groups. Thus we have a map

$$L \times N \to \mathrm{Hom}(L \otimes_K M, L \otimes_K (M \otimes_A N)),$$

given by

$$(\mu, v) \to \left(\sum_i \lambda_i \otimes u_i \to \sum_i \lambda_i \mu \otimes (u_i \otimes v) \right).$$

This map is clearly biadditive and balanced over K, and so gives a homomorphism $\theta : L \otimes_K N \to \mathrm{Hom}(L \otimes_K M,\ L \otimes_K (M \otimes_A N))$ given by

$$(\theta(\sum_j \mu_j \otimes v_j))(\sum_i \lambda_i \otimes u_i) = \sum_{i,j} \lambda_i \mu_j \otimes (u_i \otimes v_j).$$

Now consider

$$(L \otimes_K M) \times (L \otimes_K N) \to L \otimes_K (M \otimes_A N)$$

given by $(\sum_i \lambda_i \otimes u_i, \sum_j \mu_j \otimes v_j) \to (\theta(\sum_j \mu_j \otimes v_j))(\sum_i \lambda_i \otimes u_i)$. It is easy to check that it is biadditive and balanced over $L \otimes_K A$, so the universal mapping property implies that ψ is well-defined. □

1.2 Simple and semisimple modules and algebras

1.2.1 Semisimple modules. References for this section are Chs. 3 and 4 in [31], Ch. 1 in [38], and for simple rings, section 1 of Ch. 4 in [39] and §§1-5 of Ch. 8 in [65].

Theorem 1.2.1 *The following are equivalent for an R-module M:*
(a) Every submodule of M is a direct summand of M.
(b) M is the direct sum of simple submodules.
(c) M is the sum of simple submodules. □

A module with these properties is called a *semisimple* module, or a *completely reducible* module. If S is a simple R-module, the sum of all submodules of an R-module M which are isomorphic to S is a (semisimple) submodule M_S of M, called the *isotypic component* or *homogeneous component* of type S of M.

Theorem 1.2.2 *Let M be a semisimple R-module.*
(a) M is the direct sum

$$M = \oplus_S M_S$$

of its homogeneous components, (where S runs over a set of representatives of the isomorphism classes of simple R-modules). In particular, every simple submodule of M_S is isomorphic to S.
(b) If $\varphi : M \to N$ is an R-homomorphism, $\varphi M_S \subset N_S$ for all S.
(c) M_S is a direct sum of simple modules

$$M_S = \oplus_{i \in I_S} S_i$$

each isomorphic to S. The cardinalities $\{|I_S|\}$ are well-defined and determine M up to isomorphism. The length $\text{len}_R M_S$ *of M_S is finite if and only if $|I_S|$ is finite, and then* $\text{len}_R M_S = |I_S|$.
(d) Every submodule of M is semisimple. □

Lemma 1.2.1 *If N and N' are isomorphic submodules of a semisimple module M of finite length, there is a submodule Q of M such that $M = N \oplus Q = N' \oplus Q$.*

Among all submodules Q of M such that $N \cap Q = 0 = N' \cap Q$, choose one of maximal length, say Q. If $M \neq N \oplus Q$, len $M >$ len$(N \oplus Q) =$ len$(N' \oplus Q)$, so $M \neq N' \oplus Q$ as well. Since $N \oplus Q \cong N' \oplus Q$ and M has finite length, by Th. 1.2.2(c), there are isomorphic simple submodules S and S' of M such that $S \not\subset N \oplus Q$ and $S' \not\subset N' \oplus Q$. Let $S = Ru$, $S' = Ru'$ where the annihilators of u and u' are equal to the same maximal left ideal $\mathfrak{a}$ of R. If $u + u' = 0$, then $S = S'$ and $N \cap (Q \oplus S) = 0 = N' \cap (Q \oplus S)$, contradicting the maximality of Q. So $u + u' \neq 0$. Then $\mathfrak{a}$ is also the annihilator of $u + u'$, so $R(u + u') \cong R/\mathfrak{a}$ is isomorphic to S and S'. At least one of the modules $S, S', R(u+u')$ is not contained in either of $N \oplus Q$ and $N' \oplus Q$, again contradicting the maximality of Q. Therefore $M = N \oplus Q = N' \oplus Q$ as desired. □

1.2.2 Simple and semisimple rings.

Theorem 1.2.3 *The following are equivalent for a ring R:*
(a) All R-modules are semisimple.
(b) All finitely generated R-modules are semisimple.
(c) R is semisimple when considered as an R-module via left multiplication.
(d) All R-modules are projective.

(e) All short exact sequences of R-modules split. □

A *semisimple ring* R is a ring with these properties.

A finite direct product $R_1 \times \cdots \times R_n$ of semisimple rings is semisimple.

Let $M^* = \mathrm{Hom}_R(M, R)$ be the R-dual of R-module M. Let $\gamma_M : M \to M^{**}$ be the canonical mapping $u \to \langle u, \cdot\rangle$. It is an R-homomorphism.

Theorem 1.2.4 *Suppose that R is semisimple and that the R-module M has finite length.*
(a) $\mathrm{len}_R M^* = \mathrm{len}_R M$*, in particular M^* is simple if and only if M is simple.*
(b) γ_M is bijective, i.e. M is "reflexive".
(c) (i) If $M = N \oplus P$, then $M^* = N^o \oplus P^o$ and $N^o \cong P^*$ and $P^o \cong N^*$.
(ii) If $M^* = X \oplus Y$, then $M = X^o \oplus Y^o$ and $X^o \cong Y^*$ and $Y^o \cong X^*$.

If $M = M_1 \oplus M_2 \oplus \cdots \oplus M_t$, then by (1.7)

$$M^* = M_1^* \oplus M_2^* \oplus \cdots \oplus M_t^*, \tag{1.9}$$

so to prove (a) we can assume that M is simple. If $M = Ru$, the epimorphism $R \to M, r \to ru$, splits since M is projective, so there is a nonzero homomorphism $M \to R$. Thus $M^* \neq 0$.

Now let x and y be any nonzero elements of M^*. Then $x : M \to xM$ and $y : M \to yM$ are isomorphisms to the minimal nonzero left ideals xM and yM of R, and $yx^{-1} : xM \to yM$ is an isomorphism of R-modules. Since R is semisimple (and of finite length as an R-module since it is finitely generated), there are left ideals J_1 and J_2 such that $R = J_1 \oplus xM = J_2 \oplus yM$. Then $J_1 \cong J_2$ by Th. 1.2.2(c), so there is an automorphism of R as a left R-module which is yx^{-1} on xM. Such an automorphism is a right multiplication by a unit a of R, so for all $u \in M$

$$xu \to yu = (xu)a, \text{ i.e. } \langle u, y\rangle = \langle u, x\rangle a = \langle u, xa\rangle.$$

Thus $y = xa$. Since x and y are *arbitrary* nonzero elements of M^*, this implies that M^* is simple.

(b) Assume first that M is simple. Since $M^* \neq 0$ by (a), the canonical homomorphism $M \to M^{**}$ is $\neq 0$, hence must be an isomorphism since both modules are simple.

Now suppose $M = M_1 \oplus \cdots \oplus M_t$ is a decomposition of M into simple submodules. In the corresponding splitting (1.9) of M^*, M_i^* annihilates M_j if $j \neq i$. Thus the image of M_j under the canonical homomorphism γ_M annihilates all M_i^* with $i \neq j$ and so is contained in M_j^{**}, and since this map on M_j is simply γ_{M_j} itself and is $\neq 0$, it is an isomorphism and so therefore is γ_M.

(c) The first statement (i) holds without the assumption that R is semisimple – cf. p. 3. As for (ii) we can interpret M as the dual of M^* by (b), and so (ii) follows from (i). □

If X is any subset of a ring R, the *centralizer of X in R* is the subring

$$\mathrm{Z}_R(X) = \{r \in R : rx = xr \text{ for all } x \in X\}.$$

The *center* of R is the (commutative) subring $\mathrm{Z}(R) = \mathrm{Z}_R(R)$.

A ring R is *simple* if its only (2-sided) ideals are 0 and all of R.

R acts *faithfully* on a module M if $rM = 0$ implies that $r = 0$.

Theorem 1.2.5 *Let D be a division ring, and let R be the ring $\mathrm{M}(n, D)$ of $n \times n$ matrices over D. Then*

(a) R is a simple and semisimple ring. If the center of D is the field K, then the center of R is $K1_R$.

(b) There is, up to isomorphism, only one simple R-module S, namely the column vector module $D^{n\times 1}$. R acts faithfully on S and the left R-module R is isomorphic to the direct sum S^n of n copies of S.

(c) $\mathrm{End}_R S \cong D$ (if R-endomorphisms are written on the right). □

Theorem 1.2.6 Wedderburn's Theorem *for rings. If R is a semisimple simple ring, then $R \cong \mathrm{M}(n, D)$ for a uniquely determined positive integer n and division ring D (up to isomorphism), and so has, up to isomorphism, exactly one simple R-module $D^{n\times 1}$. If S is any simple R-module, $\mathrm{End}_R S \cong D$ (if endomorphisms are written on the right). As a left R-module, R is the direct sum of n simple R-modules.* □

We note also that a simple ring R is semisimple if and only if R is *Artinian*, that is to say, any chain of left ideals $I_1 \supset I_2 \supset I_3 \supset \cdots \supset I_k \supset \cdots$ is constant after a finite number of terms. A finite dimensional algebra over a field is certainly Artinian, and this is the case that is of most interest to us.

Theorem 1.2.7 *Let R be a semisimple ring.*

(a) Then

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_h$$

where the R_i are the minimal nonzero two-sided ideals of R.

(b) The R_i are simple (and semisimple) rings, are uniquely determined and are called the "simple components of R".

(c) The R_i are also the homogeneous components of R as a left R-module, and if $R_i = R_{S_i}$ (S_i a simple R-module), then S_i is the unique (up to isomorphism) simple R_i-module.

(d) If M is an R-module, then

$$M = R_1M \oplus R_2M \oplus \cdots \oplus R_hM,$$

and R_iM is the homogeneous component M_{S_i} of M. Moreover

$$M^* = \mathrm{Hom}_R(M, R) = (R_1M)^* \oplus (R_2M)^* \oplus \cdots \oplus (R_hM)^*$$

where $(R_iM)^* = \mathrm{Hom}_R(R_iM, R) = \mathrm{Hom}_{R_i}(R_iM, R_i)$. □

If $M = AM$ where A is one of the R_i or, more generally, where the ring A is a direct summand of R, we say that M is *A-isotypic*. In this case A is a direct sum of some of the R_i, and $R_jM = 0$ if $R_j \not\subset A$.

1.2.3 Simple and semisimple algebras.

All algebras from now on will be assumed finite dimensional over the field of scalars, which is usually K.

An algebra A over K is called *central* if its center $\mathrm{Z}(A) = K$ (strictly speaking $K1_A$ but we generally identify $K1_A$ with K).

Now we consider *simple* K-algebras. Since they are assumed to be of finite dimension, they are semisimple.

Theorem 1.2.8 Wedderburn's Theorem *for algebras. If A is a simple K-algebra, then $A \cong \mathrm{M}(n, D)$ for a uniquely determined positive integer n and division K-algebra D (up to isomorphism). In particular A has only one simple module, up to isomorphism.*

The map $\alpha \to \alpha \mathrm{I}_n$ is an isomorphism $\mathrm{Z}(D) \to \mathrm{Z}(\mathrm{M}(n, D))$. In particular the center of A is a field and A is a central K-algebra if and only if D is. □

The tensor product $A \otimes_K B$ of two algebras is also an algebra, with multiplication determined by $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$.

Theorem 1.2.9 *If A and B are simple K-algebras, their tensor product $A \otimes_K B$ is simple if at least one of A and B is central, and is central simple if (and only if) both are central simple. If $A \cong \mathrm{M}(m, K)$ and $B \cong \mathrm{M}(n, K)$, then $A \otimes_K B \cong \mathrm{M}(mn, K)$.* □

Proposition 1.2.1 *Let V be a finitely generated module over the simple algebra A. Then*

$$\dim_K \mathrm{Hom}_A(V, A) = \dim_K \mathrm{Hom}_K(V, K).$$

Since $\mathrm{Hom}_A(V, A)$ and $\mathrm{Hom}_K(V, K)$ are additive functors of V, we may assume that V is a simple A-module. As an A-module, A is the direct sum of copies of V, say n, so since $\mathrm{Hom}_A(A, A) = \mathrm{End}_A(A)$ consists of the right multiplications by elements of A,

$$\begin{aligned} \dim_K \mathrm{Hom}_A(V, A) &= \tfrac{1}{n} \dim_K \mathrm{Hom}_A(A, A) \\ &= \tfrac{1}{n} \dim_K A = \dim_K V = \dim_K \mathrm{Hom}_K(V, K). \end{aligned}$$ □

Theorem 1.2.10 *Suppose that A is a semisimple K-algebra and that $\mathrm{tr} : A \to K$ is a K-linear map with the properties*

1. $\mathrm{tr}(ab) = \mathrm{tr}(ba)$ for all $a, b \in A$,

2. tr is nonzero on every simple component of A.

If V is a finitely generated A-module, the map

$$\mathrm{tr}_* : \mathrm{Hom}_A(V, A) \to \mathrm{Hom}_K(V, K),$$

given by composition with tr, is an isomorphism of K-vector spaces.

By the additivity of Hom and the fact that A is semisimple, we can assume that V is simple. By Ths. 1.2.2, p. 6 and 1.2.7, the image of any A-homomorphism $V \to A$ lies in a simple component A_i of A. Since $A_j A_i$ and $A_j V$ are both 0 if A_j is some other simple component, $\mathrm{Hom}_A(V, A) = \mathrm{Hom}_{A_i}(V, A_i)$. Therefore we can also assume that A is a simple algebra.

By Prop. 1.2.1 it suffices to prove that tr_* is injective. Suppose that x is a nonzero functional in $\mathrm{Hom}_A(V, A)$. Then $x(V)$ is a minimal (nonzero) left ideal I of A. If $\mathrm{tr}\, I = 0$, then $\mathrm{tr}\, J = 0$ for all minimal left ideals J of A since by the proof of Theorem 1.2.4(a), $J = Ia$ for some $a \in A$ which implies that $\mathrm{tr} J = \mathrm{tr}(Ia) = \mathrm{tr}(aI) \subset \mathrm{tr}(I) = 0$. This contradicts the fact that $\mathrm{tr}(A) \neq 0$. Thus $\mathrm{tr}(I) \neq 0$, so $\mathrm{tr}(x(V)) \neq 0$. □

Suppose that we identify the two duals $\mathrm{Hom}_K V$ and $\mathrm{Hom}_A V$ via tr_* and denote them both by V^*. Then if we denote the corresponding pairings with V by $\langle \cdot, \cdot \rangle_K$ and $\langle \cdot, \cdot \rangle_A$,

$$\langle v, x \rangle_K = \mathrm{tr} \langle v, x \rangle_A \text{ for all } v \in V \text{ and } x \in V^*,$$

and if $\varphi \in \mathrm{Hom}_A(V, W)$,

$$\langle \varphi v, x\rangle = \mathrm{tr}\langle \varphi v, x\rangle = \mathrm{tr}\langle v, \varphi^t x\rangle = \langle v, \varphi^t x\rangle,$$

which implies

Corollary 1.2.1 *The restriction of the "K-transpose"*

$$\mathrm{Hom}_K(V, W) \xrightarrow{t} \mathrm{Hom}_K(W^*, V^*)$$

to the subgroup $\mathrm{Hom}_A(V, W)$ *of* $\mathrm{Hom}_K(V, W)$ *is the "A-transpose"*

$$\mathrm{Hom}_A(V, W) \xrightarrow{t} \mathrm{Hom}_A(W^*, V^*). \qquad \square$$

Proposition 1.2.2 *Suppose that V_1 and V_2 are left modules over the K-algebra A and W_1 and W_2 are left modules over the K-algebra B, all of them finitely generated. Write $\otimes_K = \otimes$ and assume that A and B-homomorphisms act on the right of the four modules.*
(a) There is a homomorphism

$$\mathrm{Hom}_A(V_1, V_2) \otimes \mathrm{Hom}_B(W_1, W_2) \to \mathrm{Hom}_{A\otimes B}(V_1 \otimes W_1, V_2 \otimes W_2) \tag{1.10}$$

determined by

$$\varphi \otimes \psi \to (v \otimes w \to v\varphi \otimes w\psi).$$

(b) If A and B are semisimple K-algebras, this homomorphism is an isomorphism.

(a) is straightforward.

(b) When $V_1 = V_2 = A$ and $W_1 = W_2 = B$, isomorphism is a consequence of the fact that $\mathrm{Hom}_A(A, A) \cong A$ – the right multiplications by elements of A – and the analogous isomorphisms for B and $A \otimes_K B$.

Now write $A = \oplus_i S_i$ and $B = \oplus_k T_k$ where S_i is a simple A-module for all i and T_k is a simple B-module for all k. Let $C = A \otimes_K B$. It is straightforward to check that

$$\begin{tikzcd}
\mathrm{Hom}_A(\oplus_i S_i, \oplus_j S_j) \otimes_K \mathrm{Hom}_B(\oplus_k T_k, \oplus_l T_l) \arrow[r] \arrow[d] & \mathrm{Hom}_C((\oplus_i S_i) \otimes_K (\oplus_k T_k), (\oplus_j S_j) \otimes_K (\oplus_l T_l)) \arrow[d] \\
\oplus_{i,j,k,l}(\mathrm{Hom}_A(S_i, S_j) \otimes_K \mathrm{Hom}_B(T_k, T_l)) \arrow[r] & \oplus_{i,j,k,l}\mathrm{Hom}_C(S_i \otimes_K T_k, S_j \otimes_K T_l)
\end{tikzcd}$$

is commutative, where the horizontal maps are particular cases of (1.10) and the vertical maps arise from the additivity of the functor Hom. The vertical maps are isomorphisms, and the upper horizontal map is too by the first case above, and so the lower horizontal map is also an isomorphism. This latter map is "defined component-wise",

$$\mathrm{Hom}_A(S_i, S_j) \otimes_K \mathrm{Hom}_B(T_k, T_l) \to \mathrm{Hom}_{A\otimes_K B}(S_i \otimes_K T_k, S_j \otimes_K T_l),$$

and so these component maps must also be isomorphisms. That is to say, the map (1.10) is an isomorphism when the modules are all simple, and it follows easily from this (and the additivity of Hom) that (1.10) holds in general. □

An *inner automorphism* of a ring R is an automorphism of the form $a \to cac^{-1}$ for some $c \in R^\times$. We denote it by inn_c.

Theorem 1.2.11 The Skolem-Noether Theorem. *Let A be a central simple K-algebra and B a simple K-algebra. Any two algebra homomorphisms $\varphi, \psi : B \to A$ differ by an inner automorphism of A, i.e. there is an inner automorphism ι such that the diagram*

$$\begin{tikzcd} & A \arrow[dd, "\iota"] \\ B \arrow[ur, "\varphi"] \arrow[dr, "\psi"'] & \\ & A \end{tikzcd}$$

is commutative. In particular, any algebra automorphism of A is inner. □

Theorem 1.2.12 The Centralizer Theorem. *Let A be a central simple algebra over K and B a simple subalgebra of A. Let C be the centralizer $\mathrm{Z}_A(B)$ of B. Then:*

(a) C is simple, $\mathrm{Z}(C) = \mathrm{Z}(B)$, and $\dim_K A = \dim_K B \dim_K C$.
(b) If B is central simple, then so is C and $A \cong B \otimes_K C$.
(c) $\mathrm{Z}_A(\mathrm{Z}_A(B)) = B$. □

Now let L/K be a field extension. Then $A^L := L \otimes_K A$ is an L-algebra, the *algebra obtained from A by extension of scalars to L* and its center is $L \otimes_K \mathrm{Z}(A)$; thus $L \otimes_K A$ is central if A is. Moreover $L \otimes_K A$ is a central simple L-algebra if A is a central simple K-algebra.

We will need the following elementary result.

Lemma 1.1 *Let A be a K-algebra (finite dimensional, as usual), L/K an extension of fields, and $V \subset A$ a K-vector subspace of A. Then the canonical "inclusion homomorphism" $L \otimes_K \mathrm{Z}_A(V) \to L \otimes_K A = A^L$ has image $\mathrm{Z}_{A^L}(V^L)$.*

Let $v_1, \ldots, v_n$ be a K-basis of V and let $\varphi : A \to A^n$ be the K-linear map

$$\varphi(a) = (av_1 - v_1 a, av_2 - v_2 a \ldots, av_n - v_n a).$$

The kernel of φ is $\mathrm{Z}_A(V)$ and so we have an exact sequence

$$0 \to \mathrm{Z}_A(V) \to A \xrightarrow{\varphi} A^n$$

of K-vector spaces. Since $L \otimes_K \cdot$ is an exact functor from the category of K-vector spaces to the category of L-vector spaces,

$$0 \to L \otimes_K \mathrm{Z}_A(V) \to L \otimes_K A \xrightarrow{\mathrm{id}_L \otimes_K \varphi} L \otimes_K A^n$$

is also exact. The lemma will follow if we show that the kernel of $\mathrm{id}_L \otimes_K \varphi$ is $Z_{A^L}(V^L)$. Let

$$\sum_{i=1}^{m} \lambda_i \otimes a_i \in L \otimes_K A, \quad \lambda_i \in L \quad \text{for all } i.$$

Now

$$\begin{aligned}(\mathrm{id}_L \otimes_K \varphi)\left(\sum_i \lambda_i \otimes a_i\right) &= \sum_i \lambda_i \otimes \varphi(a_i)\\ &= \sum_i (\lambda_i \otimes (a_i v_1 - v_1 a_i, a_i v_2 - v_2 a_i, \dots, a_i v_n - v_n a_i))\\ &= \sum_i (\lambda_i \otimes (a_i v_1 - v_1 a_i, 0, \dots, 0))\\ &\quad + \sum_i (\lambda_i \otimes (0, a_i v_2 - v_2 a_i, \dots, 0)) + \dots\\ &\qquad + \sum_i (\lambda_i \otimes (0, 0, \dots, a_i v_n - v_n a_i)),\end{aligned}$$

which is $= 0$ if and only if

$$\sum_i \lambda_i \otimes (a_i v_j - v_j a_i) = 0 \quad \text{for all } j,$$

if and only if

$$\left(\sum_i \lambda_i \otimes a_i\right)(1 \otimes v_j) - (1 \otimes v_j)\left(\sum_i \lambda_i \otimes a_i\right) = 0 \quad \text{for all } j,$$

if and only if

$$\sum_i \lambda_i \otimes a_i \in \mathrm{Z}_{L \otimes_K A}(L \otimes_K V) = \mathrm{Z}_{A^L} V^L. \qquad \square$$

We will also need a slight extension of the notion of scalar extension – instead of a field extension L/K, we consider a commutative K-algebra C (of finite dimension, as usual). Then $A^C = C \otimes_K A$ is a C-algebra. If C is also separable, it is a direct sum of finite separable field extensions and A^C is a semisimple respectively separable K-algebra if A is.

The simple K-algebra A is said to be *split* if $A \cong \mathrm{M}(n, K)$ for some positive integer n, and is said to be *split by* L if it is central simple and $L \otimes_K A$ is split (as an L-algebra) (and so $\cong \mathrm{M}(n, L)$ for some n). If A is split by L, then it is also split by any extension of L. A central simple algebra always has a separable splitting field of finite degree over K, and so also a Galois splitting field of finite degree. If $A \cong \mathrm{M}(n, D)$ where D is a central division algebra over K, then any maximal subfield L of D is a splitting field of D and A, and $(D : K) = (L : K)^2$.

It follows that the dimension of a central simple algebra is a square integer $(nd)^2$, where $d^2 = (D : K)$; d is called the *(Schur) index* of A and nd is the *degree* of the algebra. The degree satisfies $A^L \cong \mathrm{M}(nd, L)$ for any splitting field L of A – in particular the degree of A^L as an L-algebra is the same as that of A. In fact if A is central simple and L/K is an arbitrary field extension, the degree of A^L is the same as that of A.

The degree or index of a simple algebra is defined to be its degree or index over its center. If A is a simple K-algebra with center L_1 which is a separable field extension of K, and L_2/K is an arbitrary algebraic extension, then by Th. 1.2.15 (p. 21)

$$L_2 \otimes_K A \cong L_2 \otimes_K L_1 \otimes_{L_1} A \cong (M_1 \otimes_{L_1} A) \oplus \dots \oplus (M_m \otimes_{L_1} A)$$

for certain algebraic extensions $M_1, M_2, \ldots, M_m$ of K which contain L_1 and L_2. The degrees of the $M_i \otimes_{L_1} A$ are the same as the degree of A – thus the simple components of $L_2 \otimes_K A$ have the same degree as A.

Let A be a central simple K-algebra that it is split by the finite extension L/K. Consider A as a K-subalgebra of $L \otimes_K A$ by identifying $a = 1 \otimes a$. If $a \in A$, the trace $\operatorname{tr} a$ of a viewed as a matrix under an identification $L \otimes_K A = \mathrm{M}(nd, L)$, is independent of the identifications made and of the splitting field chosen. It is contained in K and is defined to be the *reduced trace* $\operatorname{trd} a = \operatorname{trd}_{A/K} a \in K$ of a. A similar fact holds for the determinant of $a \in A \subset \mathrm{M}(nd, L)$, which is by definition the *reduced norm* $\operatorname{nrd} a = \operatorname{nrd}_{A/K} a \in K$ of a. They have the properties

$$\begin{aligned} \operatorname{trd}(a+b) &= \operatorname{trd} a + \operatorname{trd} b & \operatorname{nrd}(ab) &= (\operatorname{nrd} a)(\operatorname{nrd} b) \\ \operatorname{trd}(\alpha a) &= \alpha \operatorname{trd} a & \operatorname{nrd}(\alpha a) &= \alpha^{nd} \operatorname{trd} a \\ \operatorname{trd}_{K_1 \otimes_K A/K_1} a &= \operatorname{trd}_{A/K} a & \operatorname{nrd}_{K_1 \otimes_K A/K_1} a &= \operatorname{nrd}_{A/K} a \\ \operatorname{trd}(ab) &= \operatorname{trd}(ba) & \operatorname{nrd}(ab) &= \operatorname{nrd}(ba) \end{aligned} \tag{1.11}$$

where $\alpha \in K$ and K_1/K is an arbitrary field extension of K.

The above relationships imply that $\operatorname{trd}(ab)$ is a symmetric bilinear form $A \times A \to K$, which can be shown to be nonsingular.

We shall also need the following lemma:

Lemma 1.2.2 *Let A and B be central simple algebras over K. Then if $a \in A$ and $b \in B$,*

$$\operatorname{trd}_{(A \otimes_K B)/K}(a \otimes b) = (\operatorname{trd}_{A/K} a)(\operatorname{trd}_{B/K} b).$$

If both A and B are split, say $A \cong \mathrm{M}(n, K)$ and $B \cong \mathrm{M}(m, K)$, then the formula holds because the "Kronecker product" $a \otimes_K b \in A \otimes_K B$ is an $nm \times nm$ matrix which can be realized as the block matrix $(a_{ij} B)$. In the general case, let L be a finite extension which splits both A and B – then it also splits $A \otimes_K B$ since

$$L \otimes_K (A \otimes_K B) \cong (L \otimes_K A) \otimes_L (L \otimes_K B),$$

and the formula follows at once. □

Except for the relation $\operatorname{nrd}(\alpha a) = \alpha^{nd} \operatorname{nrd} a$, all of the 8 properties in (1.11), as well as nonsingularity, are also enjoyed by a generalization of the reduced trace and norm to separable algebras. These are defined as follows. A *separable* K-algebra A is a semisimple K-algebra such that if

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_h$$

is its decomposition into simple algebras (cf. Th. 1.2.7), then the center K_i of each A_i is a separable field extension of K. Alternatively, it has the property that $L \otimes_K A$ is semisimple for every field extension L/K (Th. 7.18, p. 100, [55]), which implies that it is also separable for every such extension. The reduced trace and norm are then defined as

$$\operatorname{trd}_{A/K}(a) = \sum_i \mathrm{Tr}_{K_i/K} \operatorname{trd}_{A_i/K_i} a_i, \quad \operatorname{nrd}_{A/K}(a) = \prod_i \mathrm{N}_{K_i/K} \operatorname{nrd}_{A_i/K_i} a_i$$

where $a = \sum_i a_i$, $a_i \in A_i$, and $\mathrm{Tr}_{K_i/K}$ and $\mathrm{N}_{K_i/K}$ are the usual trace and norm in the field extension K_i/K. Of course each A_i is also a separable K-algebra, and we get

$$\operatorname{trd}_{A/K}(a)=\sum_i \operatorname{trd}_{A_i/K}a_i, \quad \operatorname{nrd}_{A/K}(a)=\prod_i \operatorname{nrd}_{A_i/K}a_i. \tag{1.12}$$

Suppose that $A = \mathrm{M}(n, D)$ is a separable K-algebra. If $a = (d_{ij}) \in \mathrm{M}(n, D)$ (with $d_{ij} \in D$ for all i, j), then it follows from the definition of the reduced trace and norm that

$$\operatorname{trd}_{\mathrm{A/K}}(a)=\sum_i \operatorname{trd}_{D/K}(d_{ii}) \tag{1.13}$$

and, if a is diagonal (or upper triangular),

$$\operatorname{nrd}_{\mathrm{A/K}}(a)=\prod_i \operatorname{nrd}_{D/K}(d_{ii}), \tag{1.14}$$

and that

$$\operatorname{nrd}_{A/K}A=\operatorname{nrd}_{D/K}D. \tag{1.15}$$

Exercise. Show that a commutative semisimple K-algebra is a direct sum of finite field extensions of K. □

If R is any ring – e.g. an algebra – R^o denotes the opposite ring, which $= R$ as an additive group, and whose multiplication is given by $a^o b^o = ba$, where a^o, for example, is a considered as an element of R^o. If R is a central simple algebra over K, then so is R^o.

Lemma 1.2.3 *Let A be a central simple algebra over K. Then* $\operatorname{trd}_{A^o/K}a^o = \operatorname{trd}_{A/K}a$ *and* $\operatorname{nrd}_{A^o/K}a^o = \operatorname{nrd}_{A/K}a$.

Let $o : A \to A^o$ be the antiisomorphism $a \to a^o$. It is clear that a splitting field L of A is also a splitting field of A^o. Consider the sequence of maps

$$L\otimes A \xrightarrow{\mathrm{id}\otimes o} L\otimes A^o \xrightarrow{\varphi} \mathrm{M}(nd,L) \xrightarrow{t} \mathrm{M}(nd,L)$$

where φ is an identifying isomorphism and t is transpose. We can use φ to compute $\operatorname{trd}_{A^o/K}a^o$ – namely it is $= \operatorname{tr}(\varphi(a^o))$ – and the composition of the three maps to compute $\operatorname{trd}_{A/K}a$. The image of a under the composition is simply $(\varphi(a^o))^t$, and so the statement about reduced traces follows from the fact that the matrix trace is preserved by the transpose. The proof for the reduced norm is entirely similar. □

Exercise. Suppose that $A = \mathrm{M}(n, R)$, and that

$$\varphi : A^o \to \mathrm{M}(n, R^o)$$

is the map defined by

$$\varphi\left((d_{ij})^o\right) = (d_{ij}^o)^t.$$

Show that φ is a ring isomorphism. □

There is another more elementary trace defined on a semisimple algebra – in fact defined on any finite dimensional algebra A over K – namely the "left regular algebra trace", or simply the "algebra trace". If $a \in A$, it is the trace of the K-linear transformation $x \to ax$ on A and is denoted by $\operatorname{tr}_{A/K}a$. The "left regular algebra norm" is defined similarly as $\mathrm{n}_{A/K}a = \det(x \to ax)$. The trace $\mathrm{Tr}_{L/K}$ and norm $\mathrm{N}_{L/K}$ in a finite extension L/K of fields are the regular trace and norm when L is viewed as a K-algebra.

If A is a simple separable algebra over K of degree nd, then

$$\mathrm{tr}_{A/K} a = nd\,\mathrm{trd}_{A/K} a \quad \text{for all } a \in A. \tag{1.16}$$

When A is central, see (9.17), p. 119, [55]. If A is *not* central, it follows from the fact that for *any* algebra A over L,

$$\mathrm{tr}_{A/K} = \mathrm{Tr}_{L/K} \circ \mathrm{tr}_{A/L}$$

for a subfield K of L for which L/K is finite and separable.

If G is a finite group, of order g, say, the *group algebra* KG of G is the set of all formal K-linear combinations of elements of G

$$\sum_{s \in G} \alpha_s s,$$

made into an algebra by extending the multiplication in G to all of KG using the distributive law:

$$\sum_s \alpha_s s \sum_t \beta_t t = \sum_{s,t} \alpha_s \beta_t st = \sum_r (\sum_{st=r} \alpha_s \beta_t) r.$$

KG is an (associative) algebra over K of dimension g, commutative if and only if G is.

It is clear that $\mathrm{tr}_{KG/K} s = 0$ if $s \in G,\ s \neq 1$, and $= g$ if $s = 1$, so

$$\mathrm{tr}_{KG/K} \left(\sum_{s \in G} \alpha_s s \right) = g\alpha_1.$$

Define the *canonical trace* $\mathrm{Tr}_{KG/K} = \mathrm{Tr} : KG \to K$ to be the K-linear functional such that $\mathrm{Tr}(s) = 1$ if $s = 1$, $\mathrm{Tr}(s) = 0$ otherwise. In other words

$$\mathrm{Tr}_{\mathrm{KG/K}}(\sum_{s \in G} \alpha_s s) = \alpha_1. \tag{1.17}$$

Thus

$$\mathrm{tr}_{KG/K} a = g(\mathrm{Tr}_{KG/K} a). \tag{1.18}$$

Suppose now that the characteristic of K does not divide g. We shall see later (Maschke's Theorem, Th. 1.7.1, p. 70) that KG is a separable K-algebra. Thus there is a decomposition

$$KG = A_1 \oplus A_2 \oplus \cdots \oplus A_h \tag{1.19}$$

of KG into simple algebras. There is also a simple relationship between $\mathrm{Tr}_{KG/K}$ and the reduced trace $\mathrm{trd}_{KG/K}$:

Theorem 1.2.13 *Assume that the characteristic of K does not divide g.*

(a) If $A \cong \mathrm{M}(n, D)$ is a simple component of KG, then for all $a \in A$,

$$\mathrm{Tr}_{KG/K}\, a = \tfrac{nd}{g} \mathrm{trd}_{A/K} a = \tfrac{\deg A}{g} \mathrm{trd}_{A/K} a. \tag{1.20}$$

(b) More generally, suppose that (1.19) is the decomposition of KG into simple algebras, where for each i, D_i is a division algebra of dimension d_i^2 such that $A_i \cong \mathrm{M}(n_i, D_i)$. If $a \in KG$, let $a = a_1 + \cdots + a_h$ be the decomposition of a into components $a_i \in A_i$. Then

$$\mathrm{Tr}_{KG/K}\, a = \tfrac{1}{g} \sum_i n_i d_i \mathrm{trd}_{A_i/K}\, a_i = \tfrac{1}{g} \sum_i (\deg A_i) \mathrm{trd}_{A_i/K}\, a_i.$$

Part (b) follows from (a) by the additivity of $\mathrm{Tr}_{KG/K}$. Consider (a). By (1.18) and (1.16),

$$\mathrm{Tr}_{KG/K}a = \tfrac{1}{g}\mathrm{tr}_{KG/K}a = \tfrac{1}{g}\mathrm{tr}_{A/K}a = \tfrac{1}{g}nd\,\mathrm{trd}_{A/K}. \qquad \square$$

Corollary 1.2.2 *If* $\mathrm{char}\,K \nmid g$, *then* $\mathrm{char}\,K \nmid nd$.

If a is a nonzero element of A, there is an $s \in G$ such that $\mathrm{Tr}_{KG/K}\,sa \neq 0$. Since $sa \in A$, the corollary follows from (a). □

One can also define a "reduced characteristic polynomial" $\mathrm{prd}_{A/K}a = \mathrm{prd}\,a$ for an element a in a central simple algebra A. If L is a splitting field of A, it is defined as the characteristic polynomial $\det(X\mathrm{I}_{nd} - a)$ where a is considered to be an element of $L \otimes_K A = \mathrm{M}(nd, L)$. It can be shown that it is independent of the splitting field chosen as well as the identification with $\mathrm{M}(nd, L)$, and that

$$\mathrm{prd}_{A/K}a = X^{nd} - (\mathrm{trd}_{A/K}a)X^{nd-1} + \cdots + (-1)^{nd}\mathrm{nrd}_{A/K}a \in K[X]. \qquad (1.21)$$

1.2.4 Quaternion algebras. As usual we assume here that $\mathrm{char}\,K \neq 2$. Quaternion algebras are particularly important in representation theory – see, for example, Th. 1.7.6, p. 78. They are 4-dimensional (associative) algebras A with a basis $\{1_A = 1, i, j, k\}$ and multiplication determined by two elements $\alpha, \beta \in \dot{K}$ and the rules

$$ij = k, \quad ji = -ij, \quad i^2 = \alpha \ (= \alpha 1_A), \quad j^2 = \beta.$$

It follows that i, j and k anticommute with each other, and that $k^2 = -\alpha\beta$. A is a central simple K-algebra and is denoted by $(\alpha, \beta)_K$ or simply (α, β). It is either a division algebra or is $\cong \mathrm{M}(2, K)$.

Conversely any 4-dimensional central simple algebra is a quaternion algebra.

The elements of the subspace $A_0 = Ki + Kj + Kk$ of A are called *pure quaternions*; the nonzero pure quaternions are characterized by the fact that they are not in K but their squares *are*. Thus the map * defined by $(a_0 + a_1)^* = a_0 - a_1$, where $a_0 \in K$ and $a_1 \in A_0$, is uniquely determined by the algebra structure of A, and is a (K, id)-involution[2] of A called *conjugation* (Example 6, p. 25).

The norm $\mathrm{N}_{A/K} : A \to K$ defined by $\mathrm{N}_{A/K}(a) = aa^*$ satisfies $\mathrm{N}_{A/K}(ab) = \mathrm{N}_{A/K}(a)\mathrm{N}_{A/K}(b)$. It is in fact the reduced norm $\mathrm{nrd}_{A/K}$. Similarly the map $a \to a + a^*$ is the reduced trace $\mathrm{trd}_{A/K}$, so $\mathrm{trd}_{A/K}(x_0 + x_1 i + x_2 j + x_3 k) = 2x_0$. The *norm form* of A is[3] the nonsingular quadratic form

$$\begin{aligned}\mathrm{nrd}_{A/K}(x) &= \mathrm{nrd}_{A/K}(x_0 + x_1 i + x_2 j + x_3 k)\\ &= \ x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2 = \langle 1, -\alpha, -\beta, \alpha\beta\rangle.\end{aligned}$$

A is a division algebra if and only if the norm form is anisotropic; if it is *not* a division algebra, then the norm form is $\cong \langle 1, 1, -1, -1\rangle$ which is hyperbolic.

Quaternion algebras satisfy the following fundamental identities (where $(\ ,\ ) = (\ ,\ )_K$):

(a) $(\alpha, \beta) \cong (\gamma^2\alpha, \delta^2\beta), \quad (\alpha, \beta) \cong (\beta, \alpha)$,
(b) $(1, 1) \cong \mathrm{M}(2, K) \cong (\alpha, 1) \cong (\beta, -\beta) \cong (\gamma, 1 - \gamma)$ if $\gamma \neq 0$ or 1,
(c) $(\alpha, \alpha\beta) \cong (\alpha, -\beta), \quad (\alpha, \alpha) \cong (\alpha, -1)$.

[2] Involutions are defined in §1.1 and discussed in §1.3.

[3] See §1.5.1 for these notions about forms.

(d) $(\alpha,\beta)=1$ if and only if $\alpha \in \mathrm{N}_{L/K}\dot{L}$.

Here $L=K(\sqrt{\beta})$ and, if $\beta \in \dot{K}^2$, $N_{L/K}(\gamma_1+\gamma_2\sqrt{\beta})$ is defined to be $\gamma_1^2-\gamma_2^2\beta$.

1.2.5 The Brauer group. By Wedderburn's theorem, any finite dimensional central simple K-algebra A is isomorphic to a matrix algebra $\mathrm{M}(n,D)$ where D is a central division algebra over K, *the division algebra belonging to* A. It is unique up to isomorphism. Two central simple algebras are said to be *similar* if their division algebras are isomorphic. The resulting equivalence classes are called *Brauer classes* and the collection of them is the *Brauer group* $\mathrm{Br}(K)$.

The product of two Brauer classes $[A]$ and $[B]$ in the Brauer group is the Brauer class $[A\otimes_K B]$ – the tensor product is central simple by Th. 1.2.9. The class $[K]$ of the trivial algebra K is the identity element. And the inverse of a Brauer class $[A]$ is the Brauer class $[A^o]$ of the opposite algebra A^o.

$\mathrm{Br}(K)$ is obviously Abelian, and it is also torsion: if the division algebra D in the Brauer class $[A]$ has dimension n^2, it can be shown that $[A]^n=[K]$. Thus a nonsplit quaternion algebra has order 2 in the Brauer group.

It is often more convenient to write $\mathrm{Br}(K)$ as an additive group.

Examples. 1. If K is algebraically closed, the only finite dimensional division algebra over K is K itself, so the Brauer group $\mathrm{Br}(K)=0$.

2. If $K=\mathbb{R}$ (the real numbers), or if K is a real closed field $\mathbf{R}$ (cf. §1.4), the only nontrivial division algebra over K, up to isomorphism, is the quaternion algebra $\mathbb{H}=(-1,-1)_{\mathbb{R}}$ respectively $\mathbf{H}=(-1,-1)_{\mathbf{R}}$. Thus the Brauer group $\mathrm{Br}(K)=\mathbb{Z}/2$. We can think of this isomorphism as being an injective homomorphism $\mathrm{Inv}_K : \mathrm{Br}(K)\to\mathbb{Q}/\mathbb{Z}$ with image $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$.

3. It is a theorem of Wedderburn that every finite division ring is commutative, so the Brauer group of a finite field is 0.

4. A field which is a finite extension of the field of p-adic numbers $\mathbb{Q}_p$ or of a power series field $k\langle x\rangle$ over a finite field k, is called a *local* field; it is *dyadic* if 2 is not a unit in the local ring of integers, otherwise *nondyadic*.

A local field K has a unique equivalence class of valuations, which is usually denoted by $\mathfrak{p}$ and referred to as a "prime". It induces the "$\mathfrak{p}$-adic topology" on K, under which the group of squares $\dot{K}^2$ is open (the "Local Square Theorem", p. 159, [54]).

There are several properties of local fields which are needed later. The first is (cf. p. 217, [65])

$$[\dot{K}:\dot{K}^2]=\left\{\begin{array}{cl} 4 & \text{if } K \text{ is nondyadic,} \\ 2^{2+(K:\mathbb{Q}_2)} & \text{if } K \text{ is dyadic.} \end{array}\right. \tag{1.22}$$

If K is a local field, there is a canonical isomorphism

$$\mathrm{Inv}_K : \mathrm{Br}(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

If α is a nonsquare in the local field K, then there is $\beta\in\dot{K}$ such that the quaternion algebra $(\alpha,\beta)_K$ is not split and so its image in $\mathrm{Br}(K)$ is $\neq 1$. See p. 203, [54].

We usually use the same symbol $(\alpha,\beta)_K$ – or even (α,β) – for the Brauer class of the quaternion algebra if it is unlikely to cause confusion.

Note that $\mathbb{Q}/\mathbb{Z}$ has a unique element of order 2, the Brauer class of a nonsplit quaternion algebra; thus there is, up to isomorphism, only one (central nonsplit) quaternion algebra over a local field.

Another important property of local fields is the existence of a (canonical) isomorphism $\dot{K}/\mathrm{N}_{L/K}\dot{L} \cong \mathrm{Gal}(L/K)$ if L/K is a finite Abelian extension (Th. 2.3, p. 94, [37]); in particular if L/K is a quadratic extension of local fields, then

$$[\dot{K} : \mathrm{N}_{L/K}\dot{L}] = 2. \tag{1.23}$$

5. A *global* field is either an algebraic number field (finite extension of the field $\mathbb{Q}$ of rational numbers) or a finite extension of a field $k(x)$ of rational functions over a finite field k. The completion of a global field with respect to a valuation is (isomorphic to) either a local field or, in the case of an algebraic number field, the field $\mathbb{R}$ of real numbers or the field $\mathbb{C}$ of complex numbers.

Suppose that K is a global field. To each equivalence class $\mathfrak{p}$ of valuations on K (which we usually refer to as a "prime" $\mathfrak{p}$), there corresponds a completion $K_\mathfrak{p}$. If $K_\mathfrak{p} \cong \mathbb{R}$ or $\mathbb{C}$, $\mathfrak{p}$ is called an Archimedean (or infinite) prime – more specifically a real or complex prime, while if $K_\mathfrak{p}$ is a local field, $\mathfrak{p}$ is nonArchimedean or finite.

We will need the *Approximation Theorem* (cf. p. 117, [53]):
Suppose $|\ |_1, |\ |_2, \dots, |\ |_n$ *are inequivalent valuations of the field* K *with completions* $K_1, K_2, \dots, K_n$ *respectively. If elements* $\alpha_1 \in K_1, \alpha_2 \in K_2, \dots, \alpha_n \in K_n$ *and a positive real number* ε *are given, there is an element* $\alpha \in K$ *such that* $|\alpha - \alpha_i|_i < \varepsilon$ *for* $i = 1, 2, \dots n$.

The *Global Square Theorem* (p. 182, [54]) states that a nonsquare in a global field K is a nonsquare at an infinite number of primes of K.

For each prime $\mathfrak{p}$ of a global field K, there is a homomorphism $\mathrm{Br}(K) \to \mathrm{Br}(K_\mathfrak{p})$, given by $[A] \to [A_\mathfrak{p}]$ where $A_\mathfrak{p} = K_\mathfrak{p} \otimes_K A$ – by Th. 32.1, p. 273, [55], $[A_\mathfrak{p}] = 0$ for all but a finite number of $\mathfrak{p}$. By 2. and 4. above, we get a sequence

$$0 \to \mathrm{Br}(K) \to \oplus_\mathfrak{p}\mathrm{Br}(K_\mathfrak{p}) \to \mathbb{Q}/\mathbb{Z} \to 0 \tag{1.24}$$

where the second-last map is the composite

$$\oplus_\mathfrak{p}\mathrm{Br}(K_\mathfrak{p}) \overset{\oplus_\mathfrak{p}\mathrm{Inv}_{K_\mathfrak{p}}}{\longrightarrow} \oplus_\mathfrak{p}\mathbb{Q}/\mathbb{Z} \overset{\text{add}}{\longrightarrow} \mathbb{Q}/\mathbb{Z}.$$

Here "add" means add the components of an element of $\oplus_\mathfrak{p}\mathbb{Q}/\mathbb{Z}$. This sequence is exact, and so implies in particular that for any central simple algebra A over K,

$$\sum_\mathfrak{p} \mathrm{Inv}_{K_\mathfrak{p}}[A_\mathfrak{p}] = 0,$$

the *Reciprocity Law* for K. The special case when A is a quaternion algebra $(\alpha, \beta)_K$ is often called the *Hilbert Reciprocity Law* and is usually written multiplicatively:

$$\prod_\mathfrak{p} (\alpha, \beta)_{K_\mathfrak{p}} = 1 \quad \text{for all } \alpha, \beta \in \dot{K}.$$

Equivalently, $(\alpha, \beta)_{K_\mathfrak{p}} \neq 1$ for an even number of $\mathfrak{p}$ (since in this notation, $(\alpha, \beta)_{K_\mathfrak{p}} = \pm 1$). One also sometimes writes $(\alpha, \beta)_{K_\mathfrak{p}} = (\alpha, \beta)_\mathfrak{p}$.

If S is a collection of an even number of primes of the global field K, and if $\beta \in \dot{K}$ is a nonsquare at each prime in S – that is to say, $\beta \notin \dot{K}_\mathfrak{p}^2$ for all $\mathfrak{p} \in S$ –

then there is an $\alpha \in \dot{K}$ such that $(\alpha, \beta)_\mathfrak{p} = -1$ for all $\mathfrak{p} \in S$ and is $= 1$ for all other primes. See p. 203, [54].

Lemma 1.2.4 *Let $\gamma \in \dot{K}$, an algebraic number field, and let (δ, γ) be a fixed quaternion Brauer class. Then the signs of δ at the real primes $\mathfrak{p}$ at which γ is a square (i.e. for which $\gamma >_\mathfrak{p} 0$) can be arbitrarily prescribed.*

If $\gamma \in \dot{K}^2$, the lemma is trivial, so suppose that $\gamma \notin \dot{K}^2$, and let S be the set of real primes at which γ is a square. Suppose $\varepsilon_\mathfrak{p} = \pm 1$ is given for each $\mathfrak{p} \in S$. Let $L = K(\sqrt{\gamma})$. For each $\mathfrak{p} \in S$, choose $\alpha_\mathfrak{p}, \beta_\mathfrak{p} \in K_\mathfrak{p}$ so that $(\alpha_\mathfrak{p}^2 - \beta_\mathfrak{p}^2 \gamma)\varepsilon_\mathfrak{p} > 0$. By the approximation theorem for valuations (p. 18), there are $\alpha, \beta \in K$ such that $(\alpha^2 - \beta^2\gamma)\varepsilon_\mathfrak{p} > 0$ for all $\mathfrak{p} \in S$. Since $(\mathrm{N}_{L/K}\lambda, \gamma) = 1$ for all $\lambda \in \dot{L}$ (cf. (6), 57:9, p. 146, [54]), $(\mathrm{N}_{L/K}(\alpha + \beta\sqrt{\gamma})\delta, \gamma) = (\delta, \gamma)$. □

If the Brauer class of a division algebra D has order 2, then D is a quaternion algebra if K is a local or global field; in general the index of D is a power of 2 since the index of a division algebra D and the order of $[D]$ in the Brauer group have the same prime factors (p. 254, [55]). In fact a division algebra D of order 2 in the Brauer group is similar to a tensor product of quaternion algebras by "Merkurjev's Theorem" – cf. p. 81, [39].

We will also need the following lemma in §5.5.

Lemma 1.2.5 *If L/K is a quadratic extension of global fields, the group index $[\mathrm{N}_{L/K}\dot{L} : \dot{K}^2]$ is infinite.*

Let $L = K(\sqrt{\beta})$, and let S be the set of finite primes of K at which $\beta \notin K_\mathfrak{p}^2$. S is infinite by the Global Square Theorem. If $\mathfrak{p}$ is a prime of K, the nontrivial automorphism $^-$ of L/K is continuous in the $\mathfrak{p}$-adic topology, so also the norm $\mathrm{N}_{L/K}(\lambda) = \lambda\bar{\lambda}$. Suppose $\mathfrak{p} \in S$. Then $\mathfrak{p}$ has a unique extension to L. The cosets in $(\mathrm{N}_{L_\mathfrak{p}/K_\mathfrak{p}}\dot{L}_\mathfrak{p})/\dot{K}_\mathfrak{p}^2$ are open in $\dot{K}_\mathfrak{p}$ (there are 2 of them if $\mathfrak{p}$ is nondyadic, $2^{1+(K_\mathfrak{p}:\mathbb{Q}_2)}$ if $\mathfrak{p}$ is dyadic). Let M be a positive integer, $\mathfrak{p}_1, \ldots, \mathfrak{p}_M$ distinct primes in S, and

$$(\mathrm{N}_{L_{\mathfrak{p}_i}/K_{\mathfrak{p}_i}}\lambda_i)\dot{K}_{\mathfrak{p}_i}^2 \in (\mathrm{N}_{L_{\mathfrak{p}_i}/K_{\mathfrak{p}_i}}\dot{L}_{\mathfrak{p}_i})/\dot{K}_{\mathfrak{p}_i}^2, \ \text{ for } \ i = 1, \ldots, M.$$

By the approximation theorem and the Local Square Theorem, there exists $\lambda_0 \in \dot{L}$ such that

$$(\mathrm{N}_{L_{\mathfrak{p}_i}/K_{\mathfrak{p}_i}}\lambda_0)\dot{K}_{\mathfrak{p}_i}^2 = (\mathrm{N}_{L_{\mathfrak{p}_i}/K_{\mathfrak{p}_i}}\lambda_i)\dot{K}_{\mathfrak{p}_i}^2 \ \text{ for } \ i = 1, \ldots, M. \tag{1.25}$$

Since $\mathrm{N}_{L_{\mathfrak{p}_i}/K_{\mathfrak{p}_i}}\lambda = \mathrm{N}_{L/K}\lambda$ for all $\lambda \in L$, the map $\dot{L} \to \prod_{i=1}^M (\mathrm{N}_{L_{\mathfrak{p}_i}/K_{\mathfrak{p}_i}}\dot{L}_{\mathfrak{p}_i})/\dot{K}_{\mathfrak{p}_i}^2$ given by

$$\lambda \to \Big((\mathrm{N}_{L_{\mathfrak{p}_1}/K_{\mathfrak{p}_1}}\lambda)\dot{K}_{\mathfrak{p}_1}^2, \ldots, (\mathrm{N}_{L_{\mathfrak{p}_M}/K_{\mathfrak{p}_M}}\lambda)\dot{K}_{\mathfrak{p}_M}^2\Big)$$

factors through $(\mathrm{N}_{L/K}\dot{L})/\dot{K}^2$ and so we have a map

$$(\mathrm{N}_{L/K}\dot{L})/\dot{K}^2 \to \prod_{i=1}^{M} (\mathrm{N}_{L_{\mathfrak{p}_i}/K_{\mathfrak{p}_i}}\dot{L}_{\mathfrak{p}_i})/\dot{K}_{\mathfrak{p}_i}^2$$

which is surjective by (1.25). Since M is arbitrary, the lemma follows. □

1.2.6 Compositums and tensor products of fields. A good reference is §8, pp. 99-102, [9].

Let L_1 and L_2 be extensions of K. A *compositum* or *composite extension field* of L_1 and L_2 is an extension field M/K along with K-homomorphisms $\varphi_i : L_i \to M$ such that M is generated (as a field) over K by the images $\varphi_1(L_1)$ and $\varphi_2(L_2)$. Thus a compositum is a triple

$$(M, \varphi_1, \varphi_2). \tag{1.26}$$

It is isomorphic to the compositum (N, ψ_1, ψ_2) of L_1 and L_2 if there is an isomorphism $\theta : M \to N$ such that both of the diagrams

$$\begin{tikzcd}
M \arrow[rr, "\theta"] & & N & M \arrow[rr, "\theta"] & & N \\
& L_1 \arrow[ul, "\varphi_1"] \arrow[ur, "\psi_1"'] & & & L_2 \arrow[ul, "\varphi_2"] \arrow[ur, "\psi_2"'] &
\end{tikzcd}$$

commute.

If $(M, \varphi_1, \varphi_2)$ is a compositum, there is a K-algebra homomorphism

$$(\varphi_1\varphi_2) : L_1 \otimes_K L_2 \to M$$

determined by $\varphi_1\varphi_2(\lambda_1 \otimes \lambda_2) = \varphi_1(\lambda_1)\varphi_2(\lambda_2)$. Let P be its kernel. It is a prime ideal of the commutative K-algebra $L_1 \otimes L_2$, and if $\pi_P : L_1 \otimes L_2 \to L_1 \otimes L_2/P$ is the canonical map, there is a unique homomorphism φ making the diagram

$$\begin{tikzcd}
L_1 \otimes L_2 \arrow[rr, "\varphi_1\varphi_2"] \arrow[dr, "\pi_P"'] & & M \\
& L_1 \otimes L_2/P \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

commutative. φ is an injective K-linear homomorphism of the integral domain $L_1 \otimes L_2/P$ into the field M, and has a unique K-linear extension $[\varphi] : [L_1 \otimes L_2/P] \to M$ to the field of fractions $[L_1 \otimes L_2/P]$. It makes the diagram

$$\begin{tikzcd}
L_1 \otimes L_2 \arrow[rr, "\varphi_1\varphi_2"] \arrow[dr, "\pi_P"'] & & M \\
& {[L_1 \otimes L_2/P]} \arrow[ur, "{[\varphi]}"'] &
\end{tikzcd}$$

commutative, and is an isomorphism of fields. Next consider the diagrams

$$\begin{tikzcd}
L_i \arrow[d, "\iota_i"] \arrow[drr, "\varphi_i"] & & \\
L_1 \otimes L_2 \arrow[rr, "\varphi_1\varphi_2"] \arrow[dr, "\pi_P"'] & & M \qquad (i = 1, 2) \\
& {[L_1 \otimes L_2/P]} \arrow[ur, "{[\varphi]}"'] &
\end{tikzcd}$$

where ι_1 and ι_2 are the canonical maps $\lambda_1 \to \lambda_1 \otimes 1$ and $\lambda_2 \to 1 \otimes \lambda_2$. This implies that the compositum $(M, \varphi_1, \varphi_2)$ is isomorphic to the compositum $([L_1 \otimes L_2/P], \pi_P\iota_1, \pi_P\iota_2)$, so every compositum is isomorphic to one of the latter kind.

Suppose now that P and Q are prime ideals of $L_1 \otimes L_2$, and that $([L_1 \otimes L_2/P], \pi_P\iota_1, \pi_P\iota_2)$ and $([L_1 \otimes L_2/Q], \pi_Q\iota_1, \pi_Q\iota_2)$ are isomorphic compositums:

$$\begin{tikzcd}
 & & {[L_1 \otimes L_2/P]} \arrow[dd, "\theta"'] & \\
L_i \arrow[r] \arrow[urr] \arrow[drr] & L_1 \otimes L_2 \arrow[ur, "\pi_P"] \arrow[dr, "\pi_Q"'] & & (i = 1, 2) \\
 & & {[L_1 \otimes L_2/Q]} &
\end{tikzcd}$$

are commutative. Since θ is an isomorphism,

$$Q = \ker \pi_Q = \ker \pi_P = P.$$

Thus

Theorem 1.2.14 *As P runs over the prime ideals of $L_1 \otimes L_2$,*

$$([L_1 \otimes L_2/P], \pi_P\iota_1, \pi_P\iota_2)$$

runs over a system of representatives of the isomorphism classes of compositums of L_1 and L_2. □

Proposition 1.2.3 *Suppose that L_2 is algebraic over K, and that $\hat{L}_1$ is an algebraically closed extension of L_1. Then every compositum of L_1 and L_2 is isomorphic to one of the form $(M_\varphi, \mathrm{id}_{L_1}, \varphi)$ where φ is an isomorphism of L_2 into $\hat{L}_1$ and M_φ is the subfield of $\hat{L}_1$ generated over K by L_1 and $\varphi(L_2)$.*

If $(M, \varphi_1, \varphi_2)$ is a compositum, then M is an algebraic extension of $\varphi_1 L_1$, and so the map $(\varphi_1)^{-1} : \varphi_1 L_1 \to \hat{L}_1$ has an extension to a homomorphism $\theta : M \to \hat{L}_1$. Then θ is an isomorphism of $(M, \varphi_1, \varphi_2)$ with $(M_\varphi, \mathrm{id}_{L_1}, \varphi)$ where $\varphi = \theta\varphi_2$. □

Corollary 1.2.3 *If L_1 is algebraic over K and L_2 is a finite extension of K, the number of compositums of L_1 and L_2, distinct up to isomorphism, is $\leq (L_2 : K)$.*

This follows from the proposition since the number of distinct isomorphisms of L_2 into an algebraically closed extension of K is $\leq (L_2 : K)$. □

Theorem 1.2.15 *Let $(M_j, \varphi_{j1}, \varphi_{j2})$, $1 \leq j \leq n$, be a set of representatives of the isomorphism classes of compositums of L_1 and L_2. If L_2/K is finite and separable, the homomorphism*

$$\oplus_j(\varphi_{j1}\varphi_{j2})\colon\ L_1 \otimes_K L_2 \to M_1 \oplus \cdots \oplus M_n \tag{1.27}$$

is an isomorphism of K-algebras – in fact of L_1-algebras if each M_j is made into an L_1-algebra via $\varphi_{j1} : L_1 \to M_j$. Moreover, each M_j is a finite separable extension of $\varphi_{j1} L_1$.

Since L_2 is a finite dimensional separable K-algebra, $L_1 \otimes_K L_2$ is a semisimple L_1-algebra and so is the direct sum of simple L_1-algebras by Th. 1.2.7. It must in fact be the direct sum of extension fields $N_1, \ldots, N_k$ of L_1 since it is commutative. Thus its ideals are the partial direct sums of the N_i, and its prime ideals are those of the form $\oplus_{j \neq i} N_j$. Thus by Th. 1.2.14, $n = k$ and renumbering as necessary, we can assume that the epimorphism $\varphi_{i1}\varphi_{i2}$: $L_1 \otimes L_2 \to M_i$ has kernel $\oplus_{j \neq i} N_j$, and therefore takes N_i isomorphically onto M_i. The last statement is clear. □

Corollary 1.2.4 *Suppose L_1/K and L_2/K are both finite extensions, with relatively prime degrees over K. Then if at least one of L_i/K is separable, there is only one compositum L_1L_2, up to isomorphism, and $L_1 \otimes_K L_2 \cong L_1L_2$.*

If M is a compositum, then by the multiplicativity of field degrees, $(M : K)$ is divisible by both of $(L_1 : K)$ and $(L_2 : K)$ and so $(M : K) \geq (L_1 : K)(L_2 : K)$ by the relative primeness. But $L_1 \otimes_K L_2$ has K-dimension $(L_1 : K)(L_2 : K)$, and the corollary follows at once. □

Corollary 1.2.5 *Let $\mathbf{C} = \mathbf{R}(i)$ where $\mathbf{C}/\mathbf{R}$ is a quadratic field extension with $i^2 = -1$ and $\mathbf{C}$ has involution $(\alpha + \beta i)^* = \alpha - \beta i$. Then the involution algebra $(\mathbf{C}, \mathrm{id}) \otimes_{(\mathbf{R}, \mathrm{id})} (\mathrm{M}(n, \mathbf{C}),\ {}^{t*}\ )$ is isomorphic to the (hyperbolic) involution algebra $\mathrm{M}(n, \mathbf{C}) \oplus \mathrm{M}(n, \mathbf{C})$ with the interchange involution $\overleftrightarrow{(a, b)} = (b^t, a^t)$.*

See 4, p. 24, for the tensor product of involution algebras.

If $e_{ij} \in \mathrm{M}(n, \mathbf{C})$ is the usual matrix unit, then $(\alpha \otimes \beta e_{ij})^{\mathrm{id} \otimes (t*)} = \alpha \otimes \beta^* e_{ji}$. Thus

$$(\mathbf{C}, \mathrm{id}) \otimes_{(\mathbf{R}, \mathrm{id})} (\mathrm{M}(n, \mathbf{C}),\ {}^{t*}\ ) \cong (\mathrm{M}(n, \mathbf{C} \otimes_{\mathbf{R}} \mathbf{C}),\ {}^{t-}\ )$$

where the involution ${}^{-}$ on $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C}$ is

$$\overline{\alpha \otimes \beta} = \alpha \otimes \beta^*.$$

By the theorem and Prop. 1.2.3, $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C} \cong \mathbf{C} \oplus \mathbf{C}$ via the map $\alpha \otimes \beta \to (\alpha\beta, \alpha\beta^*)$ (since the image of any $\mathbf{R}$-linear homomorphism of $\mathbf{C}$ into an algebraic closure of $\mathbf{C}$ is $\mathbf{C}$ itself). This is a homomorphism of involution algebras if the involution on $\mathbf{C} \oplus \mathbf{C}$ is the interchange involution $\overleftrightarrow{(\alpha, \beta)} = (\beta, \alpha)$, and the corollary follows. □

Corollary 1.2.6 *Assume that L_1 and L_2 are finite Galois extensions of K, with Galois groups G_1 and G_2. Let $G = G_1 \times G_2$ act as automorphisms of the K-algebra $L_1 \otimes_K L_2$ via $(\sigma_1, \sigma_2)(\lambda_1 \otimes \lambda_2) = \sigma_1\lambda_1 \otimes \sigma_2\lambda_2$, and suppose G acts on $M_1 \oplus M_2 \oplus \cdots \oplus M_n$ via the isomorphism $\oplus_j(\varphi_{j1}\varphi_{j2})$ in (1.27). If $H_j \subset G$ is the stabilizer of the direct summand M_j, the restriction map $H_j \to \mathrm{Gal}(M_j/K)$ is onto.*

Let $\sigma \in \mathrm{Gal}(M_j/K)$, and define for $i = 1, 2$

$$\sigma_i = \varphi_{ji}^{-1} \left(\sigma|_{\varphi_{ji}L_i}\right) \varphi_{ji} \in \mathrm{Gal}(L_i/K).$$

The diagrams

$$\begin{tikzcd}
M_j \arrow[rr, "\sigma"] & & M_j & M_j \arrow[rr, "\sigma"] & & M_j \\
& L_1 \arrow[ul, "\varphi_{j1}"] \arrow[ur, "\varphi_{j1}\sigma_1"'] & & & L_2 \arrow[ul, "\varphi_{j2}"] \arrow[ur, "\varphi_{j2}\sigma_2"'] &
\end{tikzcd}$$

both commute and therefore the compositums $(M_j, \varphi_{j1}, \varphi_{j2})$ and $(M_j, \varphi_{j1}\sigma_1, \varphi_{j2}\sigma_2)$ are isomorphic. This means that the action of (σ_1, σ_2) on the direct sum stabilizes M_j, i.e. $(\sigma_1, \sigma_2) \in H_j$. The commutativity of the triangles also shows that the restrictions of σ to $\varphi_{j1}L_1$ and $\varphi_{j2}L_2$ are the automorphisms induced by (σ_1, σ_2), and so σ itself must be the automorphism on M_j induced by (σ_1, σ_2) since M_j is a compositum of L_1 and L_2. □

We mention here another related fact – see Prop. 8.3, p. 164, [53]:

Theorem 1.2.16 *Let L/K be a finite separable extension. Suppose that $\mathfrak{p}$ is a prime (equivalence class of valuations, Archimedean or nonArchimedean) of K and that $\mathfrak{P}_1, \dots, \mathfrak{P}_t$ are the primes of L which lie above $\mathfrak{p}$. Then*

$$K_{\mathfrak{p}} \otimes_K L \cong L_{\mathfrak{P}_1} \oplus \cdots \oplus L_{\mathfrak{P}_t} = \oplus_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}$$

as $K_{\mathfrak{p}}$-algebras, where $K_{\mathfrak{p}}$ and $L_{\mathfrak{P}_j}$ denote completions of these fields. If $\iota_i : K_{\mathfrak{p}} \to L_{\mathfrak{P}_i}$ is the canonical map, the isomorphism is given by

$$\alpha \otimes \lambda \to ((\iota_1 \alpha)\lambda, \dots, (\iota_t \alpha)\lambda). \qquad \square$$

There is an important special case of this which arises later on – that of a quadratic extension L/K. In this case $t = 2$ or 1, so $K_{\mathfrak{p}} \otimes_K L = L_{\mathfrak{P}_1} \oplus L_{\mathfrak{P}_2}$ or $L_{\mathfrak{P}}$, depending on whether $\mathfrak{p}$ splits in L or not. In the first case $L_{\mathfrak{P}_1} = K_{\mathfrak{p}} = L_{\mathfrak{P}_2}$ and in the second, $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is a quadratic extension. Moreover it follows from the Global Square Theorem (p. 18) that the second case holds for an infinite number of $\mathfrak{p}$ when K is a global field.

Exercise. Suppose L/K is a finite Galois extension, with Galois group $G = \{\sigma_1 = 1, \sigma_2, \dots, \sigma_n\}$, and let L act on the first factor of $L \otimes_K L$ and G on the second. Suppose $\sigma \in G$ acts on $L \oplus L \oplus \cdots \oplus L$ via the permutation which takes the i^{th} component to the j^{th} where $\sigma_j \sigma = \sigma_i$. Show that the additive homomorphism

$$\varphi : L \otimes_K L \to L \oplus L \oplus \cdots \oplus L, \quad \varphi(\lambda \otimes \mu) = (\lambda\sigma_1(\mu), \lambda\sigma_2(\mu), \dots, \lambda\sigma_n(\mu)),$$

is an isomorphism of L-algebras commuting with the action of G, and that

$$\begin{tikzcd}
L \otimes_K L \arrow[r, "\varphi"] \arrow[d, "\mathrm{id}\otimes\mathrm{Tr}_{L/K}"'] & L \oplus L \oplus \cdots \oplus L \arrow[d, "\mathrm{add}"] \\
L \otimes_K K \arrow[r, "\mathrm{can}"] & L
\end{tikzcd}$$

is a commutative diagram of L-vector spaces. □

1.3 Involutions on algebras

A good treatment of this subject can be found in Ch. 8, [65], or in [36], especially §§1–8.

The center of a K-algebra $(A, {}^-)$ with involution is stable under the involution, and $(A, {}^-)$ (or the involution ${}^-$ itself) is said to be *of the first kind* if ${}^-$ is the identity on the center of A, otherwise *of the second kind*.

The *symmetric elements* respectively *skew symmetric elements* of $(A, {}^-)$ are

$$(A, {}^-)_+ = \{a \in A : \ \bar{a} = a\}, \quad (A, {}^-)_- = \{a \in A : \ \bar{a} = -a\}.$$

They are sometimes denoted simply by A_+ and A_- if the involution is clear from the context, and are the ± 1-eigenspaces of the involution viewed as a K_0-linear transformation of A. Thus

$$A = (A, {}^-)_+ \oplus (A, {}^-)_-,$$

and it is clear that the involution is determined by A_+ and A_-.

An isomorphism $\varphi : (A, {}^-) \cong (B, {}^\sim)$ of $(K, {}^-)$-involution algebras is a K-algebra isomorphism $\varphi : A \to B$ which commutes with the involutions, i.e. $\overline{\varphi(a)} = \widetilde{\varphi a}$ for all $a \in A$.

Examples. 1. The "transpose bar" $(\alpha_{ij}) \to (\bar{\alpha}_{ij})^t$ on $\mathrm{M}(n, K)$ is an involution. We usually denote it by ${}^{t-}$: $(\alpha_{ij})^{t-} = (\bar{\alpha}_{ij})^t = (\bar{\alpha}_{ji})$.

2. More generally if $(B, {}^-)$ is a $(K, {}^-)$-involution algebra, then "transpose bar"

$$(b_{ij})^{t-} = (\bar{b}_{ij})^t = (\bar{b}_{ji})$$

is a $(K, {}^-)$-involution on $\mathrm{M}(n, B)$; we write the resulting involution algebra as $\mathrm{M}(n, (B, {}^-))$ and call it the *$n \times n$ matrix (involution) algebra over* $(B, {}^-)$.

Exercise. Let $(R, {}^-)$ and $(S, {}^\sim)$ be rings with involution, and $\varphi : (R, {}^-) \to \mathrm{M}(m, (S, {}^\sim))$ a homomorphism. Define the map $\varphi_n : \mathrm{M}(n, R) \to \mathrm{M}(mn, S)$ in the obvious way, by replacing each entry r_{kl} of $(r_{ij}) \in \mathrm{M}(n, R)$ by its image $\varphi(r_{kl})$. Show that φ_n is a homomorphism $\mathrm{M}(n, (R, {}^-)) \to \mathrm{M}(mn, (S, {}^\sim))$ of rings with involution. □

3. Let b be an invertible element of a $(K, {}^-)$-involution algebra $(A, {}^-)$ satisfying $\bar{b}b^{-1} \in \mathrm{Z}(A)^\times$. Then

$$\widetilde{a} = b\bar{a}b^{-1}$$

defines another involution on A. If $\varepsilon = \bar{b}b^{-1}$, then $b = \overline{\varepsilon b} = \bar{\varepsilon}\varepsilon b$, so $\varepsilon\bar{\varepsilon} = 1$.

Suppose A is simple. Then $L = \mathrm{Z}(A)$ is a field – in fact a finite extension of K since we are assuming all algebras have finite dimension over the field of scalars. If ${}^-$ is of the first kind, $\varepsilon = \pm 1$. If ${}^-$ is of the second kind, we use Hilbert's Theorem 90 ((p. 281, [53]) to find $\eta \in L$ such that $\eta\bar{\eta}^{-1} = \varepsilon$; then if we replace b by ηb, the involution ${}^\sim$ does not change but $\bar{b} = b$; thus we can assume that $\varepsilon = 1$ in this case.

4. If $(A, {}^-)$ and $(B, {}^-)$ are $(K, {}^-)$-involution algebras, we define their sum to be

$$(A, {}^-) \oplus (B, {}^-) = (A \oplus B, {}^- \oplus {}^-),$$

and their tensor product to be

$$(A, {}^-) \otimes_{(K, {}^-)} (B, {}^-) = (A \otimes_K B, {}^- \otimes {}^-).$$

Both are involution algebras over $(K, {}^-)$ – the involution on the tensor product is given by

$$\overline{a \otimes b} = \bar{a} \otimes \bar{b}.$$

In particular if $(K, {}^-)$ is an "involution subfield" of $(L, {}^-)$ in the obvious sense, and if $(A, {}^-)$ is a $(K, {}^-)$-involution algebra, then $(L, {}^-) \otimes_{(K, {}^-)} (A, {}^-)$ is an $(L, {}^-)$-involution algebra, referred to as the involution algebra obtained from $(A, {}^-)$ by extending the scalars and sometimes denoted by $(A, {}^-)^{(L, {}^-)}$. If it is clear from the context what the involutions on K and L are, we sometimes write

$$(L, {}^-) \otimes_{(K, {}^-)} (A, {}^-) = L \otimes_K (A, {}^-).$$

Slightly more generally if $\varphi : (K, {}^-) \to (L, {}^-)$ is a homomorphism of fields with involution, one can also extend the scalars in $(A, {}^-)$ to $(L, {}^-)$ by making K act on L via $\lambda.\alpha = \lambda\varphi(\alpha)$ $(\alpha \in K, \lambda \in L)$. □

Exercises. 1. Let $(A, {}^-)$ and $(B, {}^\sim)$ be $(K, {}^-)$-involution algebras, and let $\varphi : B \otimes_K \mathrm{M}(n, A) \to \mathrm{M}(n, B \otimes_K A)$ be the canonical isomorphism of K-algebras. Show that φ is an isomorphism

$$(B, {}^\sim) \otimes_{(K, {}^-)} \mathrm{M}(n, (A, {}^-)) \to \mathrm{M}\Big(n, (B, {}^\sim) \otimes_{(K, {}^-)} (A, {}^-)\Big)$$

of involution algebras.

2. Let $(A, ^-)$ be a $(K, ^-)$-involution algebra, $(B, ^-)$ both a $(K, ^-)$ involution algebra and an $(L, ^-)$-involution algebra where the action of the fields K and L commute, and $(C, ^-)$ an $(L, ^-)$-involution algebra. Show that the canonical isomorphisms $K \otimes_K A \to A$ and $(A \otimes_K B) \otimes_L C \to A \otimes_K (B \otimes_L C)$ are also isomorphisms

$$(K, ^-) \otimes_{(K,^-)} (A, ^-) \to (A, ^-)$$
$$((A, ^-) \otimes_{(K,^-)} (B, ^-)) \otimes_{(L,^-)} (C, ^-) \to (A, ^-) \otimes_{(K,^-)} ((B, ^-) \otimes_{(L,^-)} (C, ^-)).$$

3. Let $K = K_0(\sqrt{\delta})$, with the nontrivial involution $^-$, and let $(L, ^-)$ be another involution field extension of K_0, with $L_0 = (L, ^-)_+$. Show that

$$(K, ^-) \otimes_{(K_0,\mathrm{id})} (L_0, \mathrm{id}) \cong \begin{cases} ((L_0, \mathrm{id}) \oplus (L_0, \mathrm{id}), \leftrightarrow) & \text{if } \sqrt{\delta} \in L_0, \\ (L_0(\sqrt{\delta}), ^-) = (L, ^-) & \text{if } \sqrt{\delta} \in L \setminus L_0. \end{cases}$$

Also show that

$$(K, ^-) \otimes_{(K_0,\mathrm{id})} (L, \mathrm{id}) = (L(\sqrt{\delta}), ^{-\,-})$$

if $\sqrt{\delta} \notin L$, if $^{-\,-}$ is the involution $\alpha + \beta\sqrt{\delta} \to \bar{\alpha} + \bar{\beta}(-\sqrt{\delta})$ where $\alpha, \beta \in L$.
Suggestion: use Th. 1.2.15, p. 21. □

5. If G is a finite group, the group algebra KG (cf. p. 15) has a canonical $(K, ^-)$-involution, which we also denote by $^-$, given by

$$\overline{\sum_{s \in G} \alpha_s s} = \sum_{s \in G} \bar{\alpha}_s s^{-1}.$$

It is a $(K, ^-)$-involution and we refer to it as the "standard $(K, ^-)$-involution" on KG . This is the most important involution algebra in this book.

6. Conjugation * on a quaternion algebra $A = (\alpha, \beta)_K$ is an involution of the first kind whose spaces of symmetric and skew symmetric elements are $A_+ = K1$ and $A_- = Ki + Kj + Kk = A_0$, the "pure quaternions".

If K has an involution $^- \neq$ the identity, with fixed field K_0, then the quaternion algebra $(\alpha_0, \beta_0)_K$, $\alpha_0, \beta_0 \in K_0$ is canonically isomorphic – if we consider i, j, k as given in both $(\alpha_0, \beta_0)_K$ and $(\alpha_0, \beta_0)_{K_0}$ – to $K \otimes (\alpha_0, \beta_0)_{K_0}$ and so has a canonical involution of the second kind $^- \otimes {}^*$. Conversely (cf. Th. 8.11.2(ii), p. 314, [65]), if a quaternion algebra A with center K has an involution $^\sim$ of the second kind, then it has a K_0-subalgebra A_0 which is a quaternion algebra such that

$$(A, ^\sim) \cong (K, ^-) \otimes_{(K_0,\mathrm{id})} (A_0, ^*).$$

Exercise. Determine $((\alpha_0, \beta_0)_K, ^- \otimes {}^*)_+$ and $((\alpha_0, \beta_0)_K, ^- \otimes {}^*)_-$. □

7. If $(K, ^-)$ is field with involution and A is any K-algebra, define

$$\mathrm{H}(A) = A \oplus \overline{A^o},$$

where $\overline{A^o}$ is the opposite algebra A^o with the action of K twisted by its involution (cf. p. 4). Denote by a^o the element a of A considered as an element of $\overline{A^o}$ – thus

$$\alpha a^o = (\bar{\alpha} a)^o \text{ and } a_1^o a_2^o = (a_2 a_1)^o.$$

$\mathrm{H}(A)$ has a canonical involution given by

$$\overline{(a_1, a_2^o)} = (a_2, a_1^o),$$

which is easily checked to be a $(K, {}^{-})$-involution. It is called the *hyperbolic* $(K, {}^{-})$-*involution algebra based on* A.

Note that $\mathrm{H}(A) = A \oplus \bar{A}$ where here $\bar{A}$ is the image of A under the involution ${}^{-}$ of $\mathrm{H}(A)$. Moreover it is clear that if $(B, {}^{-})$ is *any* $(K, {}^{-})$-involution algebra which has a two-sided ideal A such that $B = A \oplus \bar{A}$, then $(B, {}^{-}) \cong \mathrm{H}(A)$ and so "is" hyperbolic.

When A is a simple K-algebra, $\mathrm{H}(A)$ is a *simple involution algebra*, in the sense that the only two-sided ideals which are stable under the involution are 0 and $\mathrm{H}(A)$. By contrast a *simple algebra with involution* will mean that the algebra itself is simple – and is of course a simple involution algebra.

Conversely a simple involution algebra $(A, {}^{-})$ which is a semisimple algebra, is either simple as an algebra or a hyperbolic algebra based on a simple algebra – see p. 36.

8. Let $(B, {}^{-})$ be a $(K, {}^{-})$-involution algebra such that $B = A \oplus A'$ where the involution interchanges the two summands: $\bar{A} = A'$ and $\overline{A'} = A$. The map ${}^{-} : A' \to A$ is an isomorphism $A' \cong \overline{A^o}$ of K-algebras and $\mathrm{id}_A \oplus {}^{-} : (B, {}^{-}) \to (\mathrm{H}(A), {}^{-})$ is an isomorphism of $(K, {}^{-})$-involution algebras, so in particular $(B, {}^{-})$ is hyperbolic.

This kind of involution algebra often occurs as a direct summand of $(KG, {}^{-})$ and so plays an important role in this book.

A useful corollary of this example is that the tensor product

$$(C, {}^{-}) \otimes_{(K, {}^{-})} (\mathrm{H}(A), {}^{-})$$

is hyperbolic for any involution algebra $(C, {}^{-})$.

9. Suppose that $(B, {}^{-})$ is a $(K, {}^{-})$-involution algebra. Then $B \oplus B$ has a $(K, {}^{-})$-involution

$$(\overleftrightarrow{b_1, b_2}) = (\bar{b}_2, \bar{b}_1)$$

called the "interchange"[4]. The map $\varphi : B \to \overline{B^o}$, $\varphi(b) = (\bar{b})^o$, is an isomorphism of K-algebras, and

$$\mathrm{id} \oplus \varphi : (B \oplus B, {}^{\leftrightarrow}) \to (B \oplus \overline{B^o}, {}^{-}) = (\mathrm{H}(B), {}^{-})$$

is an isomorphism of $(K, {}^{-})$-involution algebras. Thus in this case also, $(B \oplus B, {}^{\leftrightarrow})$ is hyperbolic. (A more precise notation would be

$$((B, {}^{-}) \oplus (B, {}^{-}), {}^{\leftrightarrow}),$$

but this is usually not necessary).

An important special case is $(B, {}^{-}) = (K, {}^{-})$.

Exercise. (a) Show that

$$(K \oplus K, {}^{\leftrightarrow}) \otimes_{(K, {}^{-})} (B, {}^{-}) \cong (B \oplus B, {}^{\leftrightarrow}).$$

(b) More generally, show that if $(A, {}^{-})$ is a $(K, {}^{-})$-involution algebra,

$$(A \oplus A, {}^{\leftrightarrow}) \otimes_{(K, {}^{-})} (B, {}^{-}) \cong \big((A \otimes_{(K, {}^{-})} B) \oplus (A \otimes_{(K, {}^{-})} B), {}^{\leftrightarrow}\big)\,. \qquad \square$$

[4] The interchange involution (as it is also called in [43]) is called the "exchange involution" in [36].

Lemma 1.3.1 *Let $(L, {}^-)/(K, {}^-)$ be a (not necessarily finite) extension of involution fields, and assume $(K, {}^-) \neq (K, \mathrm{id})$. If A is a finite dimensional K-algebra, the canonical map*

$$L_0 \otimes_{K_0} A \to L \otimes_K A, \quad \lambda_0 \otimes_{K_0} a \to \lambda_0 \otimes_K a \tag{1.28}$$

is an isomorphism of L_0-algebras. Furthermore if $(A, {}^-)$ is a $(K, {}^-)$-involution algebra, (1.28) is an isomorphism

$$(L_0, \mathrm{id}) \otimes_{(K_0, \mathrm{id})} (A, {}^-) \cong (L, {}^-) \otimes_{(K, {}^-)} (A, {}^-)$$

of involution algebras.

Since $L_0 \otimes_{K_0} A$ and $L \otimes_K A$ have the same finite L_0-dimension, in order to prove that (1.28) is an isomorphism of L_0-vector spaces, it suffices to show that it is onto. Let $K = K_0(\sqrt{\delta})$. Then $L = L_0(\sqrt{\delta})$, and $(\alpha_0 + \beta_0\sqrt{\delta}) \otimes a$ $(\alpha_0, \beta_0 \in L_0)$ is the image of $\alpha_0 \otimes a + \beta_0 \otimes \sqrt{\delta} a$. That it is an isomorphism of involution algebras is easily checked. □

1.3.1 Involutions on simple algebras. Suppose now that A is a central simple K-algebra. Then there is a converse to Example 3 above, namely

10. Let ${}^-$ and ${}^\sim$ be $(K, {}^-)$-involutions on A. Their composition $\bar{\tilde{\ }}$ is a K-automorphism of A, hence by the Skolem-Noether Theorem (Th. 1.2.11) it is an inner automorphism, say $a \to bab^{-1}$. This implies that $\widetilde{a} = \bar{b}^{-1}\bar{a}\bar{b}$, and that $b^{-1}\bar{b} \in \dot{K}$ since ${}^\sim$ is an involution. As we saw in Example 3, this implies that $\bar{b} = \varepsilon b$ where $\varepsilon = \pm 1$ if ${}^-$ is of the first kind, and we can assume that $\varepsilon = 1$ if ${}^-$ is of the second kind. □

Suppose that A is central simple over K of dimension n^2 and has a $(K, {}^-)$-involution. Then there are precisely 3 possibilities for the dimensions of A_+ and A_- (cf. Th. 8.7.5, p. 303, [65]):

(a) If the involution is of the second kind, then

$$\dim_{K_0} A_+ = \dim_{K_0} A_- = n^2,$$

and the involution and the involution algebra $(A, {}^-))$ are said to be *unitary* or *of unitary type*. (If $(B, {}^-)$ is a simple algebra with involution, we also say that the hyperbolic simple involution algebra $(B \oplus B, \leftrightarrow)$ is unitary).

(b) If the involution is of the first kind and

$$\dim_K A_+ = \tfrac{1}{2}n(n+1), \quad \dim_K A_- = \tfrac{1}{2}n(n-1),$$

the involution and the involution algebra $(A, {}^-)$ are said to be *orthogonal* or *of orthogonal type*.

(c) If the involution is of the first kind and

$$\dim_K A_+ = \tfrac{1}{2}n(n-1), \quad \dim_K A_- = \tfrac{1}{2}n(n+1),$$

the involution and the involution algebra $(A, {}^-)$ are said to be *symplectic* or *of symplectic type*.

If the involution is of the second kind, say $K = K_0(\sqrt{\delta})$, then multiplication by $\sqrt{\delta}$ interchanges the K_0-spaces A_+ and A_-, and so (a) follows at once from $A = A_+ \oplus A_-$.

In the case of an involution of the *first* kind, this is shown as follows: If $A = \mathrm{M}(n, K)$, by Examples 1 and 10 above the involution is of the form $\bar{a} = ba^tb^{-1}$

for some $b \in \mathbf{GL}(n, K)$ satisfying $b^t = \varepsilon b$ with $\varepsilon = \pm 1$. The condition $\bar{a} = a$ is equivalent to $(ab)^t = \varepsilon ab$, and it follows easily that its eigenspaces A_+ and A_- have the dimensions in (b) if $\varepsilon = 1$, i.e. if b is symmetric, and have the dimensions in (c) if $\varepsilon = -1$, i.e. if b is skew symmetric. (This shows of course how the terminology in (b) and (c) arises). The bilinear form[5] $\hat{b}(u, v) = u^t bv$ on $K^{n\times 1}$ is nonsingular and ε-symmetric, and it is easy to see that $^-$ is the *adjoint* with respect to $\hat{b}$, namely

$$\hat{b}(au, v) = \hat{b}(u, \bar{a}v) \quad \text{for all } \ a \in A,$$

(cf. (1.34), p. 46). If A is *not* split, the K-dimensions of the eigenspaces A_+ and A_- will of course be the same as the L-dimensions of $(A^L)_+$ and $(A^L)_-$ for any splitting extension L/K, namely those given in (b) and (c).

As examples, the identity on K and the transpose on $\mathrm{M}(n, K)$ are orthogonal involutions.

If A is simple but not necessarily central over K, $(A, ^-)$ is called *orthogonal, symplectic* or *unitary* if it is such over its center. The simple involution algebra $\mathrm{H}(B)$ based on the simple K-algebra B will also be called unitary. Thus if $(A, ^-)$ is a simple involution algebra, it is unitary if and only if $^-$ is not the identity on its center.

Theorem 1.3.1 *Let $(D, ^-)$ be a (possibly split) quaternion algebra over K with an involution of the first kind. The involution is symplectic if and only if it is conjugation. The conjugate transpose on $\mathrm{M}(n, D)$ is also symplectic.*

For a symplectic involution, D_+ and D_- have dimensions 1 and 3 respectively. Thus it is clear that conjugation on D is symplectic.

Conversely suppose $^-$ is any symplectic involution on the central quaternion K-algebra D. Since $^-$ is the identity on $K1_D$, $D_+ = K1_D$. On the other hand the 3-dimensional subspace $Ki + Kj + Kk$ of pure quaternions is stable under $^-$ since it is $= \{a \in D : \ a \notin \dot{K}, \ a^2 \in K\}$. Thus it must $= D_-$ and so the involution is conjugation.

The last statement is a special case of the following lemma:

Lemma 1.3.2 *Let $(A, ^-)$ be a central simple algebra with involution over $(K, ^-)$. Then the type of $\mathrm{M}(r, (A, ^-))$ is the same as that of $(A, ^-)$.*

Clearly the "kind" is the same, so $(A, ^-)$ unitary implies that $\mathrm{M}(r, (A, ^-))$ is unitary. Suppose that $(A, ^-)$ is orthogonal and $\dim_K A = n^2$. Then the dimension of the "diagonal elements" fixed under $^{t-}$ + the dimension of the "off-diagonal elements" fixed by it is

$$r\tfrac{1}{2}n(n+1) + \tfrac{1}{2}r(r-1)n^2 = \tfrac{1}{2}rn(rn+1),$$

which implies that $\mathrm{M}(r, (A, ^-))$ is orthogonal since its dimension is $(rn)^2$. The proof for the symplectic case is similar. □

Exercises. 1. Let A be a central simple algebra over K with a $(K, ^-)$-involution. Say that the involution (or $(A, ^-)$) *has type* 1 if the involution is orthogonal, *type* -1 if it is symplectic, and *type* 0 if it is unitary. Show that the type of $(A^o, ^-)$ is the same as that of $(A, ^-)$, and if $(B, ^-)$ is another central simple algebra with a $(K, ^-)$-involution, that the type of $(A, ^-) \otimes_{(K,^-)} (B, ^-)$ is (type of $(A, ^-)$)(type of $(B, ^-)$).

[5] The basic notions of bilinear and sesquilinear forms are given in §1.5.1.

2. Show that the index of a simple algebra with an involution of the first kind is a power of 2. (Use the fact ([55], p. 254) that the exponent of A (its order in $\mathrm{Br}(\mathrm{Z}(A))$) and its index have the same prime factors).

3. Let $(\mathrm{M}(2,K),{}^-)$ be a symplectic involution algebra. Suppose that D is a quaternion algebra over K and that $\varphi : D \to \mathrm{M}(2,K)$ is an isomorphism of K-algebras. Show that φ is also an isomorphism $(D,\ ^*\ ) \to (\mathrm{M}(2,K),{}^-)$ of involution algebras. □

4. If $(A,{}^-)$ is symplectic, show that its degree is even.

Lemma 1.3.3 *Let $(A,{}^-)$ be a $(K,{}^-)$-involution algebra with A simple, and $(M,{}^-)/(K,{}^-)$ an extension of fields with involution. Suppose that*

$$(A^M,{}^-) = (M,{}^-) \otimes_{(K,{}^-)} (A,{}^-)$$

and that

$$A^M = B \oplus \bar{B} \oplus \cdots \tag{1.29}$$

where B (and $\bar{B}$) are simple algebras. Let V be an A-module (finitely generated, as usual). Then

$$\mathrm{len}_{A^M} BV^M = \mathrm{len}_{A^M} \bar{B}V^M. \tag{1.30}$$

We may assume that V is simple. Suppose that $B \cong \mathrm{M}(n,D)$, so $\mathrm{len}_{A^M} B = n$. Since $\bar{B} \cong B^o$ and $B^o \cong \mathrm{M}(n,D^o)$, $\mathrm{len}_{A^M}\bar{B}$ is also $= n$. Thus if we view (1.29) as the decomposition of the left A^M-module A^M into isotypic components, the isotypic components B and $\bar{B}$ have the same length as A^M-modules. On the other hand $V^m \cong A$ (as an A-module) for some m, so $(V^M)^m \cong A^M = B \oplus \bar{B} \oplus \cdots$, and therefore its isotypic components of type S_B (a simple B-module) and of type $S_{\bar{B}}$ have the same length, and therefore the same must be true of V^M, i.e. (1.30) holds. □

Theorem 1.3.2 *Let $(A,{}^-)$ be a separable simple $(K,{}^-)$-involution algebra and $(M,{}^-)/(K,{}^-)$ an extension of involution fields of the same kind. Then the simple (involution) factors of $(M,{}^-) \otimes_{(K,{}^-)} (A,{}^-)$ are separable M-algebras and have the same type as $(A,{}^-)$.*

Suppose first that $(A,{}^-)$ is hyperbolic, say $A = B \oplus \bar{B}$. Then B is a simple separable K-algebra. So $M \otimes_K B$ is semisimple and therefore is a direct sum of simple M-algebras. If L is the center of B, the center $M \otimes_K L$ of $M \otimes_K B$ is a direct sum of finite separable extensions of M since L/K is finite and separable (Th. 1.2.15, p. 21). and it follows that $(M,{}^-) \otimes_{(K,{}^-)} (A,{}^-)$ is a direct sum of simple separable hyperbolic M-algebras.

Therefore we may assume that A is simple (and separable). Then $M \otimes_K A$ is semisimple and so a direct sum of simple $(M,{}^-)$-involution algebras which are also separable as M-algebras by the foregoing argument. If L is the center of A, the center of $M \otimes_K A$ is

$$M \otimes_K L = L_1 \oplus \cdots \oplus L_k$$

where the L_i are finite separable extensions of M (*ibid*), and are the centers of the simple components of $M \otimes_K A$:

$$M \otimes_K A \cong (M \otimes_K L) \otimes_L A \cong (L_1 \otimes_L A) \oplus \cdots \oplus (L_k \otimes_L A).$$

If $1 \le i \le k$, the involution ${}^- \otimes {}^-$ of $M \otimes_K A$ either stabilizes $L_i \otimes_L A$ or interchanges it with $L_j \otimes_L A$ for some $j \ne i$. Thus $(M,{}^-) \otimes_{(K,{}^-)} (A,{}^-)$ is a direct sum of separable simple involution algebras, and we must show that they are all of the same type as A.

If $(A, ^-)$ is unitary, the involution is nontrivial on its center L. Then either the involution interchanges $L_i \otimes_L A$ with $L_j \otimes_L A$, $j \neq i$, or $L_i \otimes_L A$ is stable and the involution is nontrivial on L_i since

$$L \to M \otimes_K L = L_1 \oplus \cdots \oplus L_k \xrightarrow{\text{proj.}} L_i$$

is a homomorphism of involution algebras. This proves the theorem in the unitary case (since hyperbolic algebras are considered to be unitary).

Suppose then that $(A, ^-)$ is orthogonal or symplectic. Since $(M, ^-)$ has the same kind as $(K, ^-)$ – namely the first kind – the involution on $M \otimes_K L$ is the identity, so also on each L_i. Thus $A_i = L_i \otimes_L A$ is stable under the involution and it follows immediately that

$$\dim_{L_i}(A_i)_+ = \dim_L A_+ \text{ and } \dim_{L_i}(A_i)_- = \dim_L A_- \text{ for all } i,$$

whence the theorem. □

Theorem 1.3.3 *Let A and B be central simple algebras over K which are similar. Then A admits a $(K, ^-)$-involution if and only if B admits a $(K, ^-)$-involution. In particular if A has a $(K, ^-)$-involution, then so does the division algebra D such that $A \cong \mathrm{M}(n, D)$.*

See Corollary 8.3, p. 306, [65]. □

Theorem 1.3.4 *Let A be a central simple K-algebra with a $(K, ^-)$-involution, and B a simple subalgebra of A with a $(K, ^-)$-involution $^\sim$. Then $^\sim$ can be extended to an involution on A.*

This is Th. 10.1, p. 311 in [65]. Th. 4.14, p. 51, [36] is a somewhat sharper form of this theorem, giving the possible types of the extension. □

Theorem 1.3.5 *Let A be a simple separable K-algebra with an involution $^-$ of the first kind. If K is a global field and $K_\mathfrak{p}$ is the completion of K at a prime $\mathfrak{p}$, then $(K_\mathfrak{p}, \mathrm{id}) \otimes_{(K,\mathrm{id})} (A, ^-)$ is a direct sum of involution algebras of the same type (orthogonal or symplectic) as $(A, ^-)$ – namely if $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ are the primes of the center L of A lying above $\mathfrak{p}$, and for each i, $^-$ denotes the extension of the involution on A to an involution of the first kind on $A_{L_{\mathfrak{P}_i}}$, then*

$$(A_{K_\mathfrak{p}}, ^-) \cong (A_{L_{\mathfrak{P}_1}}, ^-) \oplus \cdots \oplus (A_{L_{\mathfrak{P}_t}}, ^-).$$

By Th. 1.2.16, there is a canonical isomorphism $K_\mathfrak{p} \otimes_K L \cong L_{\mathfrak{P}_1} \oplus \cdots \oplus L_{\mathfrak{P}_t}$. Thus

$$K_\mathfrak{p} \otimes_K A \cong (K_\mathfrak{p} \otimes_K L) \otimes_L A \cong (L_{\mathfrak{P}_1} \otimes_L A) \oplus \cdots \oplus (L_{\mathfrak{P}_t} \otimes_L A).$$

Since the involution on $K_\mathfrak{p} \otimes_K L$ is the identity, the involution on the right side stabilizes all of the summands, and so the theorem follows by dimensions – for example, $\dim_{L_{\mathfrak{P}_i}}(L_{\mathfrak{P}_i} \otimes_L A)_+ = \dim_L A_+$ – or by Ex. 1 on p. 29. □

Theorem 1.3.6 *Let A be a central simple algebra with two $(K, ^-)$-involutions $^-$ and $^\sim$.*

(a) Then $\widetilde{a} = b^{-1}\bar{a}b$ for some $b \in A$ such that $\bar{b} = \pm b$; if $^-$ is of the second kind, then b can be chosen so that $\bar{b} = b$.

(b) If $(A, ^-)$ is orthogonal, then the involution $^\sim$ is orthogonal if $\bar{b} = b$, symplectic if $\bar{b} = -b$.

(c) *If* $(A, {}^-)$ *is symplectic, then the involution* ${}^\sim$ *is symplectic if* $\bar{b} = b$, *orthogonal if* $\bar{b} = -b$.

Part (a) is Example 10 above.

Suppose $\bar{b} = \varepsilon_0 b$ where $\varepsilon_0 = \pm 1$. Since $\widetilde{a} = \varepsilon a$ if and only if $\overline{ba} = \varepsilon_0 \varepsilon ba$, i.e. $a \in b^{-1} A^{(-)}_{\varepsilon_0 \varepsilon}$, $\dim_K A^{(\sim)}_{\varepsilon} = \dim_K A^{(-)}_{\varepsilon_0\varepsilon}$ (where $A^{(-)}_{+}$, for example, is the space of elements of A which are symmetric with respect to ${}^-$). Thus the dimensions of the eigenspaces A_+ and A_- of ${}^\sim$ are the same as those of the corresponding eigenspaces of ${}^-$ if $\varepsilon_0 = 1$, and are interchanged if $\varepsilon_0 = -1$. □

Exercise. Let $(A, {}^-)$ be a simple algebra with an involution of the first kind, and let $(B, {}^-) = \mathrm{M}(n, (A, {}^-))$. Suppose that ${}^\sim$ is a second involution of the first kind on B, and that $b_0 \in B^\times$ satisfies $\widetilde{b} = b_0 \bar{b} b_0^{-1}$ for all $b \in B$. Show that $\bar{b}_0 = \varepsilon_0 b_0$ where $\varepsilon_0 = \pm 1$, and that

$$\mathrm{type}(B, {}^\sim) = \varepsilon_0 \mathrm{type}(A, {}^-). \qquad \square$$

Corollary 1.3.1 (cf. Prop. 7.1, p. 81, [36]) *Let A be a central simple K-algebra of even degree with an orthogonal involution* ${}^-$. *If $a, b \in A_-$ are invertible elements of A, then* $\mathrm{nrd}\, a \equiv \mathrm{nrd}\, b \bmod \dot{K}^2$.

The involution $\widetilde{x} = a\bar{x}a^{-1}$ is symplectic by the theorem, and $\widetilde{ab} = ab$. Therefore it suffices to show that $\mathrm{nrd}\, c \in K^2$ for all $c \in A^{(\sim)}_+$. We do this by showing that the reduced characteristic polynomial $\mathrm{prd}_A c$ is a square in $K[X]$. The result then follows from (1.21), since the degree nd is even.

Let L be a Galois splitting field of A, $L \otimes_K A \cong \mathrm{M}(nd, L)$. It suffices to show that $\mathrm{prd}_A c$ is a square in $L[X]$, since the monic square root of $\mathrm{prd}_A c$ is invariant under the Galois group of L/K since $L[X]$ is a unique factorization domain, and so must be in $K[X]$. Therefore we can assume that A is split, $A = \mathrm{M}(n, K)$.

Since transpose is an orthogonal involution, there is a skew symmetric matrix r (in the usual sense, i.e. with respect to the transpose) so that $\widetilde{x} = rx^t r^{-1}$ for all $x \in A$. Let A_- denote the subspace of skew symmetric matrices, of dimension $\frac{1}{2}n(n-1)$. Then rA_- consists of matrices which are symmetric with respect to ${}^\sim$, and since it also has dimension $\frac{1}{2}n(n-1)$ and ${}^\sim$ is symplectic, it must be the *entire* space $A^{(\sim)}_+$ of matrices which are symmetric with respect to ${}^\sim$. Therefore there is $e \in A_-$ such that $c = re$, and so

$$\mathrm{prd}_A c = \det(X\mathrm{I}_n - c) = (\det r)\det(Xr^{-1} - e).$$

Since r and $Xr^{-1} - e$ are skew-symmetric, $\det r$ and $\det(Xr^{-1} - e)$ are squares, in $\mathrm{M}(n, K)$ and $\mathrm{M}(n, K[X])$ respectively, of their Pfaffians (cf. p. 45). □

This corollary makes it possible to define the determinant $\det_K({}^-)$ and discriminant $\mathrm{disc}_K({}^-) = (-1)^{nd/2}\det_K({}^-)$ of an orthogonal involution ${}^-$ on a separable simple K-algebra of *even* degree nd:

$$\det_K({}^-) = (\mathrm{nrd}_{A/K} a)\dot{K}^2 \in \dot{K}/\dot{K}^2, \quad \text{where } a \in A_- \cap A^\times$$

(cf. p. 81, [36]). If A is central simple, the determinant and discriminant are well-defined by the corollary, and if it is separable simple, say with center L, then they are well defined since $\mathrm{nrd}_{A/K} = \mathrm{N}_{L/K}\mathrm{nrd}_{A/L}$.

This definition will be used in Ch. 5 in the case of $A = \mathrm{M}(n, D)$ where D is either the field L or a quaternion algebra over K. In the latter case $\bar{a} = h_0^{-1} a^{t*} h_0$ where $h_0^{t*} = -h_0$ by Th. 1.3.6(c), and so

$$\det_K(^-) =_2 \mathrm{nrd}_{A/K} h_0$$

since $\bar{h}_0 = -h_0$ also. Suppose that $A = \mathrm{M}(n, K)$. Note that $\det_K(^t) =_2 1$ since a skew symmetric matrix has square determinant (cf. p. 45). Write $\bar{a} = h_0^{-1} a^t h_0$ where $h_0^t = h_0$ (Th. 1.3.6(b)). Then it is straightforward to check that

$$A_-^{(-)} = h_0^{-1} A_-^{(t)},$$

whence

$$\det_K(^-) =_2 \mathrm{nrd}_{A/K} h_0^{-1} =_2 \mathrm{nrd}_{A/K} h_0.$$

This formula also holds when $A = \mathrm{M}(n, L)$ where L/K is a finite separable extension.

Two further definitions for orthogonal involutions used in Ch. 5 are of the Hasse and Hasse-Witt invariants, albeit in more special circumstances, namely when A is split of even degree and $\mathrm{disc}(^-) = 1$ for the Hasse invariant, and when A is split of odd degree in the case of the Hasse-Witt invariant. Thus when $A \cong \mathrm{M}(n, K)$, $\mathrm{disc}(^-) = 1$ and n is even, we define

$$\mathrm{s}(^-) = \mathrm{s}(\langle h_0 \rangle). \tag{1.31}$$

(See p. 53 for the definition of the Hasse invariant $\mathrm{s}(b)$ of a symmetric bilinear form.) This is well-defined since, by Prop. 1.5.1(a) (p. 53), if $\alpha \in \dot{K}$

$$\begin{aligned} \mathrm{s}(\langle \alpha h_0 \rangle) &= \mathrm{s}(\langle h_0 \rangle)(\alpha, -1)_K^{n(n-1)/2} (\alpha, \det h_0)_K^{n-1} \\ &= \mathrm{s}(\langle h_0 \rangle)(\alpha, \mathrm{disc}\, h_0)_K = \mathrm{s}(\langle h_0 \rangle). \end{aligned}$$

If K is a global field and $\mathfrak{p}$ a prime of K, $\mathrm{s}_{\mathfrak{p}}(^-)$ stands for the Hasse invariant $\mathrm{s}(^-)$ of the involution of $\mathrm{M}(n, K_{\mathfrak{p}})$.

If $A \cong \mathrm{M}(n, K)$, and n is odd, we define the Hasse-Witt invariant

$$\mathrm{w}(^-) = \mathrm{w}(\langle h_0 \rangle).$$

This is well-defined by Lem. 1.5.2, p. 55. In fact it is also well-defined when n is even and $\mathrm{disc}(^-) = 1$.

If it is necessary to make the field K explicit, we will of course write $\mathrm{s}_K(^-)$ and $\mathrm{w}_K(^-)$.

One can similarly define the determinant of a unitary involution $^-$ on a simple separable K-algebra $A \cong \mathrm{M}(n, D)$ when n itself is even: identify A with $\mathrm{M}(n, D)$ and write $\bar{a} = h_0^{-1} a^{t-} h_0$, where $^-$ also denotes an $(L, ^-)$-involution on D, L is the center of A (and D), and $h_0^{t-} = h_0$ (possible by Hilbert's Theorem 90 – cf. p. 24). By Lem. 1.3.7 (p. 34), $\mathrm{nrd}_{A/K} h_0 \in \dot{K}_0$. Define

$$\det_K(^-) = (\mathrm{nrd}_{A/K} h_0) \mathrm{N}_{K/K_0} \dot{K} \in \dot{K}_0 / \mathrm{N}_{K/K_0} \dot{K}.$$

Lemma 1.3.4 *Let $(K, ^-)$ be of the second kind. If $(A, ^-)$ is a separable simple K-algebra $\cong \mathrm{M}(n, D)$ with n even and $(K, ^-)$-involution $^-$, then $\det_K(^-)$ is well-defined.*

It suffices to prove the lemma when A is central simple since $\mathrm{nrd}_{A/K} = \mathrm{N}_{L/K} \circ \mathrm{nrd}_{A/L}$ and, by Lem. 1.3.5 below, $\mathrm{N}_{L/K}L_0 \subset \mathrm{K}_0$ where L_0 and K_0 are, as usual, the fixed elements of L and K under the involution.

Fix the identification $A = \mathrm{M}(n, D)$ for the moment. Any other choice of h_0 is of the form αh_0 where $\alpha \in \dot{K}$. But $\alpha h_0 = (\alpha h_0)^{t-} = \bar{\alpha} h_0^{t-} = \bar{\alpha} h_0$ and so $\alpha \in \dot{K}_0$. Let $\hat{K}$ be a splitting field of D, so $\hat{K} \otimes_K \mathrm{M}(n, D) \cong \mathrm{M}(nd, \hat{K})$ where $\dim_K D = d^2$. Under this isomorphism, $\alpha \mathrm{I}_n \in \mathrm{M}(n, D)$ corresponds to $\alpha \mathrm{I}_{nd}$, and so $\mathrm{nrd}_{A/K}\alpha \mathrm{I}_n = \alpha^{nd}, \in \mathrm{N}_{K/K_0}\dot{K}$ since $K_0^2 \subset \mathrm{N}_{K/K_0}K$ and nd is even. Thus $\det_K(-)$ is independent of the choice of h_0.

Suppose $(A, {}^-) \to (\mathrm{M}(n, D), {}^{t-}\mathrm{inn}_{g_0^{-1}})$, $g_0^{t-} = g_0$, is another identification. It gives rise to an isomorphism

$$\mathrm{inn}_c : (\mathrm{M}(n, D), {}^{t-}\mathrm{inn}_{g_0^{-1}}) \to (\mathrm{M}(n, D), {}^{t-}\mathrm{inn}_{h_0^{-1}})$$

of involution algebras, which implies that

$$cg_0^{-1}a^{t-}g_0c^{-1} = h_0^{-1}(cac^{-1})^{t-}h_0 = h_0^{-1}(c^{-1})^{t-}a^{t-}c^{t-}h_0 \text{ for all } a \in \mathrm{M}(n, D),$$

and this in turn implies that, for some $\alpha \in \dot{K}$,

$$\alpha g_0 c^{-1} = c^{t-}h_0, \text{ i.e. } \alpha g_0 = c^{t-}h_0 c.$$

But $(c^{t-}h_0c)^{t-} = c^{t-}h_0c$ so $\alpha \in \dot{K}_0$. Also $\mathrm{nrd}_{A/K}(c^{t-}) = \overline{\mathrm{nrd}_{A/K}c}$ by Lem. 1.3.7, and so

$$\mathrm{nrd}_{A/K}g_0\mathrm{N}_{K/K_0}\dot{K} = \mathrm{nrd}_{A/K}h_0\mathrm{N}_{K/K_0}\dot{K}.$$

Thus $\det({}^-)$ does not depend on the identification $A = \mathrm{M}(n, D)$.

It remains to show that it is also independent of the choice of the involution ${}^-$ on D. Suppose ${}^\sim$ is another $(K, {}^-)$-involution on D, say $\widetilde{d} = c\bar{d}c^{-1}$ for all $d \in D$. Again we can assume that $\bar{c} = c$ by Hilbert's Theorem 90, so $\mathrm{nrd}_{D/K}c \in \dot{K}_0$. If $a = (d_{ij}) \in \mathrm{M}(n, D)$,

$$\begin{aligned} \bar{a} = h_0^{-1}(d_{ij})^{t-}h_0 &= h_0^{-1}(\bar{d}_{ji})h_0 \\ &= h_0^{-1}(c^{-1}\widetilde{d}_{ji}c)h_0 = (c\mathrm{I}_nh_0)^{-1}(d_{ij})^{t\sim}(c\mathrm{I}_nh_0). \end{aligned}$$

Again using the splitting field $\hat{K}$ to calculate reduced norms, we see that

$$\mathrm{nrd}_{A/K}(c\mathrm{I}_n) = (\mathrm{nrd}_{D/K}c)^n$$

and so

$$\mathrm{nrd}_{A/K}(c\mathrm{I}_nh_0)\mathrm{N}_{K/K_0}\dot{K} = (\mathrm{nrd}_{D/K}c)^n(\mathrm{nrd}_{A/K}h_0)\mathrm{N}_{K/K_0}\dot{K} = (\mathrm{nrd}_{A/K}h_0)\mathrm{N}_{K/K_0}\dot{K}$$

since n is even and $\mathrm{nrd}_{D/K}c \in \dot{K}_0$. □

Lemma 1.3.5 *If L/K is a finite separable extension and ${}^-$ is an involution on L such that $\bar{K} = K$, then*

$$\mathrm{Tr}_{L/K}\bar{\lambda} = \overline{\mathrm{Tr}_{L/K}\lambda} \quad \textit{and} \quad \mathrm{N}_{L/K}\bar{\lambda} = \overline{\mathrm{N}_{L/K}\lambda}.$$

This is a simple exercise, using the definition of $\mathrm{Tr}_{L/K}$ and $\mathrm{N}_{L/K}$ in terms of the trace and determinant of multiplication $\alpha \to \lambda\alpha$ on L – and the fact that if $\omega_1, \ldots, \omega_l$ is a basis of L/K, then so is $\bar{\omega}_1, \ldots, \bar{\omega}_l$. □

Lemma 1.3.6 *Suppose A is a central simple K-algebra with $(K, ^-)$-involutions $^\sim$ and $^-$. Then $(A, ^\sim) \cong (A, ^-)$ if and only if there is a unit $b \in A^\times$ such that $\widetilde{a} = (b\bar{b})\bar{a}(b\bar{b})^{-1}$ for all $a \in A$.*

Suppose the involution algebras are isomorphic: by the Skolem-Noether Theorem, there is $b \in A^\times$ such that

$$b^{-1}\widetilde{a}b = \overline{b^{-1}ab} = \bar{b}\bar{a}\bar{b}^{-1} \quad \text{for all } a \in A.$$

This proves the necessity and the sufficiency is also clear from this expression. □

Theorem 1.3.7 *Let A be a central simple K-algebra.*

(a) ("Albert's Theorem") A admits an involution of the first kind if and only if it is isomorphic to its opposite algebra A^o, i.e. the Brauer class of A has order 1 or 2.

(b) [6] If the involution on K is $\neq$ the identity, A admits an involution of the second kind if and only if the "corestriction" $\operatorname{Cor} A$ over the fixed field K_0 splits.

(c) If A admits a $(K, ^-)$-involution, then every algebra similar to A (in particular the division algebra in the Brauer class of A) admits a $(K, ^-)$-involution.

See p. 306, 8.8.3, 8.8.4, and p. 309, 8.9.5, in [65], or Th. 3.1, p. 31, [36]. □

If K is a local field, a (noncommutative) division algebra D over K does not admit an involution of the second kind (Theorem 2.2 (ii), p. 353, [65]). Furthermore the only noncommutative central division algebra over K with an involution of the *first* kind is the quaternions. In fact any such algebra is isomorphic to its opposite algebra and so of order 2 in the Brauer group; and since the latter is $\cong \mathbb{Q}/\mathbb{Z}$ (cf. p. 17), there is only one element of order 2.

Lemma 1.3.7 (2.2 and 2.16, [36]) *Let $(A, ^-)$ be a simple separable K-algebra with a $(K, ^-)$-involution. Then*

$$\overline{\operatorname{trd}_{A/K} a} = \operatorname{trd}_{A/K} \bar{a}, \quad \overline{\operatorname{nrd}_{A/K} a} = \operatorname{nrd}_{A/K} \bar{a}.$$

Suppose first that K is the center of A. Let M be a splitting field of A which is Galois over the subfield K_0 of K of elements fixed by $^-$, and $\varphi : M \otimes_K A \to \mathrm{M}(n, M)$ an M-isomorphism. Choose $\sigma \in \operatorname{Gal}(M/K_0)$ which restricts to $^-$ on K. Then

$$M \times A \to M \otimes_K A, \quad (\lambda, a) \to \sigma(\lambda) \otimes \bar{a},$$

is biadditive and balanced over K, so we get a homomorphism

$$\Sigma : M \otimes_K A \to M \otimes_K A, \quad \Sigma(\lambda \otimes a) = \sigma(\lambda) \otimes \bar{a},$$

of Abelian groups. It is in fact a σ-linear anti-automorphism of M-algebras. Now consider

$$\begin{tikzcd}
M \otimes A \arrow[r, "\Sigma"] \arrow[d, "\varphi"'] & M \otimes A \arrow[r, "i"] & M \otimes A^o \arrow[d, dotted, "\psi"] \\
\mathrm{M}(n, M) \arrow[rr, "\hat{\sigma}"] & & \mathrm{M}(n, M)
\end{tikzcd}$$

where $\hat{\sigma}$ is the map which applies σ to every entry of the matrix, and $i(\lambda \otimes a) = \lambda \otimes a^o$. Since the four undotted maps are bijective, there is a unique map ψ making the diagram commutative; it is an isomorphism of M-algebras. Thus $\psi(1 \otimes a^o) =$

[6] This part is not used in this book, so we will not define "corestriction".

$\hat{\sigma}\varphi\Sigma^{-1}i^{-1}(1\otimes a^o) = \hat{\sigma}\varphi(1\otimes\bar{a})$, and so since the matrix trace $\mathrm{tr}(\varphi(1\otimes\bar{a})) = \mathrm{trd}_{A/K}\bar{a}$ lies in K,

$$\begin{aligned}\overline{\mathrm{trd}_{A/K}\bar{a}} = \overline{\mathrm{tr}(\varphi(1\otimes\bar{a}))} &= \sigma(\mathrm{tr}(\varphi(1\otimes\bar{a}))) \\ &= \mathrm{tr}(\hat{\sigma}\varphi(1\otimes\bar{a})) = \mathrm{tr}(\psi(1\otimes a^o)) \\ &= \mathrm{trd}_{A^o/K}a^o = \mathrm{trd}_{A/K}a.\end{aligned}$$

The last step follows from Lem. 1.2.3, p. 14.

If A is not central, one applies Lem. 1.3.5 to the central case just proved. □

The property $\overline{\mathrm{trd}_{A/K}a} = \mathrm{trd}_{A/K}\bar{a}$ is important in the subject of isometry representations, and we make the following definition:

Definition 1.3.1 *If $(A, ^-)$ is a $(K, ^-)$-involution algebra, an involution trace*

$$\mathrm{t} : (A, ^-) \to (K, ^-)$$

is a K-linear map $\mathrm{t} : A \to K$ which commutes with the involutions:

$$\mathrm{t}(\bar{a}) = \overline{\mathrm{t}(a)} \quad \textit{for all } a \in A,$$

is symmetric – i.e. $\mathrm{t}(ab) = \mathrm{t}(ba)$ for all $a, b \in A$ – and is nonsingular in the sense that the (symmetric or Hermitian) form $\mathrm{t}(a,b) = \mathrm{t}(a\bar{b})$ on A is nonsingular.

The form $\mathrm{t}(a,b)$ is called the *trace form* of the algebra A/K – or more precisely of the involution trace t. (The basic properties of symmetric and Hermitian forms are dealt with in §1.5).

Examples 1. To show that $\mathrm{t} = \mathrm{trd}_{A/K}$ is an involution trace when A is a separable algebra, we begin with the simple case. It remains to check that t is nonsingular since symmetry follows by (1.11), p. 13. It suffices to show that it is nondegenerate ($\mathrm{t}(A,a) = 0 \Rightarrow a = 0$) since this means that the right adjoint $\mathrm{t}_r : A \to \overline{A^*}$ is injective and therefore bijective. The kernel

$$\{a \in A : \mathrm{t}(Aa) = 0\}$$

is a two-sided ideal $\neq A$ and so must be 0, hence $\mathrm{trd}_{A/K}$ is indeed nonsingular.

Now suppose that $(A, ^-)$ is a separable algebra such that $A = B \oplus \bar{B}$ where B is a simple K-algebra. By Example 8, p. 26, $(A, ^-)$ is hyperbolic, and by the foregoing argument, the right adjoint t_r is injective on both B and $\bar{B}$, and since it takes them to $(\bar{B})^*$ and B^* respectively, it is injective on A itself. Thus $\mathrm{t} = \mathrm{trd}_{A/K}$ is an involution trace in this case too.

It follows now that the reduced trace is also an involution trace when A is a separable K-algebra. For in this case $(A, ^-)$ is a direct sum of separable simple algebras with $(K, ^-)$-involutions and separable hyperbolic algebras – see the next section.

2. If $(L, ^-)/(K, ^-)$ is a finite separable extension of fields with involution, then $\mathrm{Tr}_{L/K}$ is an involution trace – this is a special case of Example 1.

3. Let $A = KG$ with the standard $(K, ^-)$-involution. Then the canonical trace

$$\mathrm{Tr}_{KG/K}(\sum_s \alpha_s s) = \alpha_1$$

is an involution trace. It is clear that it commutes with the involutions and symmetry follows from

$$\mathrm{Tr}_{KG/K}\left((\sum_s \alpha_s s)(\sum_s \beta_s s)\right) = \sum_s \alpha_s \beta_{s^{-1}}.$$

Nonsingularity results from the fact that G is an orthonormal basis of KG with respect to $\mathrm{Tr}(a\bar{b})$: if $s, t \in G$, $\mathrm{Tr}(s\bar{t}) = 1$ if $s = t$ and $= 0$ if $s \neq t$. It also follows from Example 1 and Th. 1.2.13 (p. 15).

4. Suppose that $\mathrm{t} : (A, {}^-) \to (K, {}^-)$ is an involution trace, and that the involution algebra $(B, {}^-)$ is a direct summand of $(A, {}^-)$. Then $\mathrm{t}|_B : (B, {}^-) \to (K, {}^-)$ is an involution trace. Only the last property of involution trace needs verification; and this is clear since if $(A, {}^-) = (B, {}^-) \oplus (C, {}^-)$, then as reflexive spaces over $(K, {}^-)$, $A = B \perp C$ with respect to the nonsingular form $\mathrm{t}(a, a')$. □

1.3.2 Involutions on semisimple algebras. Now suppose that A is a semisimple K-algebra with $(K, {}^-)$-involution ${}^-$. Let

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_h$$

be the decomposition of A into its simple (algebra) components (cf. Th. 1.2.7). Since $\bar{A}_i$ is also a minimal nonzero 2-sided ideal of A, hence one of the A_j, the involution permutes these simple algebras, and so A is the direct sum of two kinds of algebras – those A_i which are stable under the involution, and algebras of the form $A_i \oplus \bar{A}_i$. Thus these components of A, in either case, are simple $(K, {}^-)$-involution algebras (cf. p. 26). An algebra of the form $A_i \oplus \bar{A}_i$ is (isomorphic to) the hyperbolic (involution) algebra $\mathrm{H}(A_i)$ by Ex. 8, p. 26.

In particular a simple involution algebra $(A, {}^-)$ which is semisimple as an algebra, is either a simple algebra or a hyperbolic algebra $\mathrm{H}(B)$ on a simple algebra B.

Therefore after a possible renumbering of the A_i, we get a splitting

$$(A, {}^-) = (A_1, {}^-) \oplus \cdots \oplus (A_k, {}^-) \oplus \mathrm{H}(A_{k+1}) \oplus \cdots \oplus \mathrm{H}(A_l)$$

into simple involution algebras. These direct summands are called the *simple (involution) components* of $(A, {}^-)$. This will generally be written as (with another change in notation)

$$(A, {}^-) = (A_1, {}^-) \oplus \cdots \oplus (A_k, {}^-) \oplus (A_{k+1}, {}^-) \oplus \cdots \oplus (A_l, {}^-) \qquad (1.32)$$

where now $A_1, \ldots, A_k$ are still simple algebras and $(A_{k+1}, {}^-), \ldots, (A_l, {}^-)$ are simple involution algebras which are hyperbolic.

1.4 Formally real fields

A *formally real field* is a field in which -1 is *not* a sum of squares. In this case we say that the *level* of K, $s(K)$, is ∞. If K is *not* formally real, the level is the least integer n such that -1 is a sum of n squares in K.

If K is a finite field with q elements, then

$$s(K) = \begin{cases} 1 & q \equiv 1 \bmod 4 \text{ or is a power of 2,} \\ 2 & q \equiv 3 \bmod 4, \end{cases}$$

(cf. p.71, [65]). Thus a formally real field has characteristic 0.

Let K be a local field. By Examples 2.4, p. 380, [39], if p is the characteristic of its residue class field,

$$s(K) = \begin{cases} 1 & p \equiv 1 \bmod 4 \text{ or } \sqrt{-1} \in K, \\ 2 & p \equiv 3 \bmod 4 \text{ and } \sqrt{-1} \notin K, \\ 4 & p = 2,\ (K : \mathbb{Q}_2) \text{ odd}, \\ 2 & p = 2,\ (K : \mathbb{Q}_2) \text{ even and } \sqrt{-1} \notin K, \end{cases}$$

It is a theorem of A. Pfister (p. 379, *ibid*) that the level of a field is a power of 2 or ∞.

An *ordering* of the field K is a subset $P \subset \dot{K}$ such that

(a) $\alpha, \beta \in P$ implies $\alpha + \beta \in P$.

(b) $\alpha, \beta \in P$ implies $\alpha\beta \in P$.

(c) $P \cup -P = \dot{K}$

Note that $P \cap (-P) = \emptyset$ since if α were in the intersection, then α and $-\alpha \in P$, so $0 = \alpha - \alpha \in P$.

An *ordered field* is a field K with a given ordering P – more formally a pair (K, P). The elements of P are called positive and those of $-P$ negative. An ordering in the usual sense of the word is defined by saying that $\alpha > \beta$ if $\alpha - \beta \in P$. It has the familiar properties:

$\alpha, \beta > 0$ implies that $\alpha + \beta$ and $\alpha\beta$ are > 0.
If $\alpha, \beta \in K$, then either $\alpha < \beta, \alpha = \beta$, or $\alpha > \beta$.
$\alpha > \beta > \gamma$ implies that $\alpha > \gamma$.
$\alpha > \beta,\ \gamma > 0$ implies that $\alpha\gamma > \beta\gamma$.
$\alpha \neq 0$ implies that $\alpha^2 > 0$.

If it is not clear from the context which ordering P is being used to define $>$, we write $\alpha >_P \beta$ or say that $\alpha > \beta$ at P.

Details on orderings and formally real fields can be found in [65], especially §4, §6 and §10 of Ch. 2, and Ch. 3, and also in Ch. VIII, [39]. We list here some of their basic properties:

1. Suppose K is ordered. Then any sum of squares $\sum \alpha_i^2 + 1^2$ is $\in P$, hence is nonzero, so -1 is not a sum of squares. Thus an ordered field is formally real. The converse is also true:

Theorem 1.4.1 Artin-Schreier. *A formally real field has at least one ordering. The set of all sums of squares of nonzero elements of a formally real field K is the intersection $\cap P$ of all orderings of K.* □

2. Let P be an ordering on K, and let $b : V \times V \to K$ be a nonsingular symmetric bilinear form. Choose an orthogonal basis $v_1, v_2, \ldots, v_n$ for V over K. Let $r^+(b) =$ the number of $b(v_j, v_j)$ which are > 0 at P, and $r^-(b) =$ the number which are < 0. Thus $r^+(b) + r^-(b) = n$. Define the *signature* of b (at P) to be $\text{sgn}(b) = \text{sgn}_P(b) = r^+(b) - r^-(b)$.

Theorem 1.4.2 Inertia Theorem of Jacobi and Sylvester. $\text{sgn}_P(b)$ *is independent of the basis used to define it.* □

The positive index $r^+(b)$ and the negative index $r^-(b)$ are also independent of the choice of basis. b is called *positive definite* if $r^+(b) = n$, i.e. if $r^-(b) = 0$ or if $\text{sgn}_P(b) = n$, and *negative definite* if $r^-(b) = n$ or $\text{sgn}_P(b) = -n$.

3. The rationals $\mathbb{Q}$ and reals $\mathbb{R}$ have only one ordering, the usual ones.

4. The field K is called *Euclidean* if the set of nonzero squares $\dot{K}^2$ is an ordering of K – and therefore the *only* ordering of K. In particular then any sum of squares is a square. When K is Euclidean, two nonsingular symmetric bilinear forms are equivalent if and only if their ranks and their signatures are equal (cf. 4.8, p. 42, [65]). And the signature provides an isomorphism

$$\operatorname{sgn}_{\dot{K}^2} : \mathrm{W}_1(K) \to \mathbb{Z}$$

of the Witt ring.

5. If K has an ordering P, it can be extended to the field $K(x)$ of rational functions. For example we can define $f(x)/g(x)$ to be positive if $f(x)g(x)$ has positive leading coefficient. This implies then that the ordering on K can be extended to *any* purely transcendental extension. □

A formally real field K is *real closed* if no proper algebraic extension of K is formally real. This is the same as saying that there is no extension of an ordering on K to any proper algebraic extension. In this case the set of nonzero squares $\dot{K}^2$ is an ordering in K, so in particular a real closed field is Euclidean (3.1.14, p. 111, [65]) and remark 4. above applies.

An extension $\mathbf{R}$ of a formally real field K is a *real closure* of K if it is real closed and algebraic over K. It follows from Zorn's Lemma that, if P is an ordering of K, there is a real closure $\mathbf{R}$ in any algebraically closed extension whose ordering $\dot{\mathbf{R}}^2$ is an extension of P – i.e. $P = \dot{\mathbf{R}}^2 \cap K$; it is called a real closure of K at P.

If $\mathbf{R}$ is real closed, $\mathbf{R}(i)$, where $i^2 = -1$, is an algebraic closure of $\mathbf{R}$. If K_P is a real closure of K at P, $K_P(i)$ is called an *algebraic closure of K at P*.

Theorem 1.4.3 (Artin-Schreier) *If $\mathbf{R}_1$ and $\mathbf{R}_2$ are real closures for the same ordering of the field K (so $K \cap \dot{\mathbf{R}}_1^2 = K \cap \dot{\mathbf{R}}_2^2$), there is a unique K-isomorphism $\mathbf{R}_1 \cong \mathbf{R}_2$.* □

Real closures $\mathbf{R}_1$ and $\mathbf{R}_2$ for *different* orderings P_1 and P_2 of K cannot be K-isomorphic, since such an isomorphism would carry the ordering $\dot{\mathbf{R}}_1^2$ onto the ordering $\dot{\mathbf{R}}_2^2$, and hence the orderings $\dot{\mathbf{R}}_1^2 \cap K = P_1$ and $\dot{\mathbf{R}}_2^2 \cap K = P_2$ would be equal. Thus there is a canonical bijection between the orderings of K and the K-isomorphism classes of real closures of K.

Theorem 1.4.4 *(p. 113, ibid) The following are equivalent:*

(a) K is real closed.

(b) K is Euclidean and every polynomial of odd degree in $K[X]$ has a zero in K.

(c) K is not algebraically closed but $K(\sqrt{-1})$ is. □

Theorem 1.4.5 *If $\mathbf{C}$ is an algebraically closed field of characteristic $\neq 2$ which has an automorphism of order 2, then the fixed field of the automorphism is a real closed field $\mathbf{R}$, and $\mathbf{C} = \mathbf{R}(i)$ where $i^2 = -1$.*

Since $(\mathbf{C} : \mathbf{R}) = 2$, $\mathbf{R}$ contains nonsquares; let δ be one of them. Then $\mathbf{C} = \mathbf{R}(\sqrt{\delta})$. Let $\alpha + \beta\sqrt{\delta}$ $(\alpha, \beta \in \mathbf{R})$ be a fourth root of δ in $\mathbf{C}$. Then $\alpha \neq 0 \neq \beta$ and

$$(\alpha + \beta\sqrt{\delta})^4 = (\alpha^4 + 6\alpha^2\beta^2\delta + \beta^4\delta^2) + 4\alpha\beta(\alpha^2 + \beta^2\delta)\sqrt{\delta} \in \mathbf{R}.$$

This implies that $\alpha^2 + \beta^2\delta = 0$, so $\delta = -\frac{\alpha^2}{\beta^2} \in -\dot{\mathbf{R}}^2$. Thus $\mathbf{R}$ is the union of its squares and their negatives, and $-1 \notin \dot{\mathbf{R}}^2$.

We next show that $P = \dot{\mathbf{R}}^2$ is an ordering on $\mathbf{R}$. First of all $P \cap -P = \emptyset$ since otherwise we would have an equality $\beta^2 = -\gamma^2$ with $\beta, \gamma \in \dot{\mathbf{R}}$, which is impossible since -1 is not a square in $\mathbf{R}$. Of course $PP \subset P$, so it remains to show that $P + P \subset P$, in other words the sum of 2 nonzero squares $\alpha^2 + \beta^2$ is a square. Consider the polynomial

$$\begin{aligned} & (x + \sqrt{\alpha + \beta i})(x - \sqrt{\alpha + \beta i})(x + \sqrt{\alpha - \beta i})(x - \sqrt{\alpha - \beta i}) \\ = \;& (x^2 - (\alpha + \beta i))(x^2 - (\alpha - \beta i)) \\ = \;& x^4 - 2\alpha x^2 + (\alpha^2 + \beta^2) \in \mathbf{R}[x]. \end{aligned}$$

Since neither $\alpha + \beta i$ nor $\alpha - \beta i$ is in $\mathbf{R}$ and since the maximum degree of an irreducible polynomial in $\mathbf{R}[x]$ is 2, the irreducible factors of this polynomial over $\mathbf{R}$ must be of degree 2. And so at least one of the polynomials

$$\begin{aligned} (x + \sqrt{\alpha + \beta i})(x + \sqrt{\alpha - \beta i}) &= x^2 + (\sqrt{\alpha + \beta i} + \sqrt{\alpha - \beta i})x + \sqrt{\alpha^2 + \beta^2}, \\ (x + \sqrt{\alpha + \beta i})(x - \sqrt{\alpha - \beta i}) &= x^2 + (\sqrt{\alpha + \beta i} - \sqrt{\alpha - \beta i})x - \sqrt{\alpha^2 + \beta^2} \end{aligned}$$

is an irreducible polynomial over $\mathbf{R}$. It follows that $\sqrt{\alpha^2 + \beta^2} \in \mathbf{R}$, i.e. that $\alpha^2 + \beta^2$ is a square in $\mathbf{R}$.

Therefore $\mathbf{R}$ is formally real and so is real closed since its only algebraic extension is $\mathbf{C} = \mathbf{R}(i)$. □

There is in fact a much stronger theorem, also due to E. Artin and O. Schreier – see 2.21, p. 250, [39]:

Theorem 1.4.6 *If* $\mathbf{C}$ *is algebraically closed and* K *is a proper subfield of finite codimension* $(\mathbf{C} : K)$*, then* char $\mathbf{C} = 0$*,* K *is real closed, and* $\mathbf{C} = K(\sqrt{-1})$ *(so* $(\mathbf{C} : K) = 2$*).* □

Lemma 1.4.1 *Suppose that* $\mathbf{R}$ *is real closed, and let* $\mathbf{C} = \mathbf{R}(\sqrt{-1})$*, its algebraic closure. Let* ζ *be a primitive* n^{th} *root of unity in* $\mathbf{C}$*. Then if* * *is the nonidentity automorphism of* $\mathbf{C}/\mathbf{R}$*,* $\zeta^* = \zeta^{-1}$*.*

We may suppose that $n > 2$. Let $\eta \in \mathbf{C}$, $\eta^2 = \zeta$. Now $\eta\eta^* = \mathrm{N}_{\mathbf{C}/\mathbf{R}}\eta \in \mathbf{R}$ and $(\eta\eta^*)^2$ is an n^{th} root of unity; if $(\eta\eta^*)^2 \neq 1$, then

$$((\eta\eta^*)^2)^{n-1} + ((\eta\eta^*)^2)^{n-2} + \cdots + (\eta\eta^*)^2 = -1$$

which is impossible. Therefore $\zeta\zeta^* = (\eta\eta^*)^2$ must be 1. □

If $L = K(\theta)$ is an algebraic extension of K and the minimal polynomial of θ over K is $p(X)$, then the number of extensions of an ordering P on K to L is the number of zeros of p in a real closure K_P, and is also equal to the number of K-imbeddings of L into K_P (cf. 3.2.7 and 3.2.8, pp. 115-116, [65]). Thus the number of extensions of a given ordering is $\leq (L : K)$; if the number is actually $= (L : K)$ for the ordering P, L/K is called a *totally real* extension at P, and if it is $= (L : K)$ for *every* ordering of K (and K is formally real), L/K is called a *totally real* extension. If P is an ordering of K for which no extension to L/K is possible, then L/K is called an *imaginary* extension at P, and if this is true for *all* P (in other words, L is not formally real but K is), then L/K is called a *totally imaginary* extension.

Theorem 1.4.7 *Let P be an ordering of K, $\mathbf{R}$ a real closure of K at P, and $\mathbf{C} = \mathbf{R}(i)$ its algebraic closure. If $L = K(\theta)$ is a finite extension, then*

$$\mathbf{R} \otimes_K L = \overbrace{\mathbf{R} \oplus \cdots \oplus \mathbf{R}}^{r} \oplus \overbrace{\mathbf{C} \oplus \cdots \oplus \mathbf{C}}^{s}$$

where r is the number of conjugates of θ in $\mathbf{R}$ (and therefore $2s$ is the number in $\mathbf{C} \setminus \mathbf{R}$). In particular P has $(L : K)$ extensions to L (i.e. L/K is totally real at P) if

$$\mathbf{R} \otimes_K L = \mathbf{R} \oplus \cdots \oplus \mathbf{R},$$

and has no extensions (i.e. L/K is imaginary at P) if

$$\mathbf{R} \otimes_K L = \mathbf{C} \oplus \cdots \oplus \mathbf{C}.$$

Apply Prop. 1.2.3 (p. 21) with $L_2 = L$, $L_1 = \mathbf{R}$ and $\hat{L}_1 = \mathbf{C}$: the compositums $M_1, \ldots, M_t$ of L and $\mathbf{R}$ are of the form $\varphi L \cdot \mathbf{R}$ (the subfield of $\mathbf{C}$ generated by φL and $\mathbf{R}$) where φ runs over the $t = r + 2s$ imbeddings $L \to \mathbf{C}$ – which correspond to the conjugates of θ in $\mathbf{C}$. By Th. 1.2.15 (p. 21), the imbeddings of $\mathbf{R}$ and L into their composites give rise to an isomorphism

$$\mathbf{R} \otimes_K L \xrightarrow{\sim} M_1 \oplus \cdots \oplus M_t,$$

and it is clear that $M_i = \mathbf{R}$ or $\mathbf{C}$, and $= \mathbf{R}$ if and only the corresponding conjugate of θ is in $\mathbf{R}$.

Alternatively one can apply the functor $\mathbf{R} \otimes_K$ to the exact sequence

$$0 \to (p(X)) \to K[X] \to L \to 0$$

where $(p(X))$ is the principal ideal generated by the minimal polynomial $p(X) \in K[X]$ of θ over K, giving the exact sequence

$$0 \to (p(X)) \to \mathbf{R}[X] \to \mathbf{R} \otimes_K L \to 0$$

where $(p(X))$ is now the principal ideal in $\mathbf{R}[X]$. One now factors $p(X)$ into irreducibles

$$p(X) = l_1(X) \ldots l_{r_1}(X) q_1(X) \ldots q_{r_2}(X)$$

in $\mathbf{R}[X]$, where the l_i are linear and the q_i quadratic, and applies the Chinese Remainder Theorem to obtain

$$\begin{aligned} \mathbf{R} \otimes_K L &\cong \mathbf{R}[X]/(l_1 \ldots l_{r_1} q_1 \ldots q_{r_2}) \\ &\cong \big(\oplus_i \mathbf{R}[X]/(l_i) \big) \oplus \big(\oplus_i \mathbf{R}[X]/(q_i) \big). \end{aligned}$$ □

Corollary 1.4.1 *If (K_0, P) is an ordered field and $\delta \in \dot{K}_0 \setminus \dot{K}_0^2$, then P can be extended to the quadratic extension $K = K_0(\sqrt{\delta})$ if and only if $\delta >_P 0$.*

Since the ordering of a real closure $\mathbf{R}$ at P is $\dot{\mathbf{R}}^2$ and $P = \dot{\mathbf{R}}^2 \cap K_0$, $\delta >_P 0$ if and only if δ is a square in $\mathbf{R}$ if and only if $\mathbf{R}[X]/(X^2 - \delta) = \mathbf{R} \oplus \mathbf{R}$. So the corollary follows from the second part of Th. 1.4.7. □

It turns out that the case when an ordering *cannot* be extended is more important later on (cf. §4.10) in the situation of a field $(K, {}^-)$ with involution (with subfield $K_0 = (K, {}^-)_+$ of symmetric elements). If P is an ordering of K_0, we will say that ${}^-$ is a *definite involution at P* if $a\bar{a} >_P 0$ for all $a \in \dot{K}$, or that K/K_0 is a *definite extension at P*; this is equivalent to saying that either $K = K_0$ (and P is an ordering of K), or that $K = K_0(\sqrt{\delta})$ with $\delta < 0$ at P. The involution ${}^-$

is *definite* – or K/K_0 is a definite extension – if there *is* an ordering P of K_0 at which K/K_0 is definite, and it is *totally definite* if K_0 is formally real and K/K_0 is definite at each ordering of K_0.

If $^-$ or K/K_0 is not definite at P and $K \neq K_0$, we call it *indefinite at P*. If $K \neq K_0$ and K/K_0 is indefinite at each ordering P, or if $K = K_0$ and K_0 is not formally real, K/K_0 is simply called *indefinite*. In particular, K/K_0 is indefinite if K/K_0 is a totally real quadratic extension.

If K/K_0 is a definite quadratic extension at P and $h : V \times V \to (K, ^-)$ is an Hermitian form, the positive and negative indices $r^+(h)$ and $r^-(h)$ are again defined using an orthogonal basis of (V, h), exactly as in the case of a symmetric bilinear form, and the signature $\operatorname{sgn}(h) = \operatorname{sgn}_P(h)$ is defined to be $r^+(h) - r^-(h)$. That they are well-defined follows from the symmetric bilinear case since if $\alpha \in \dot{K}_0$ and $\langle \alpha \rangle$ is the corresponding Hermitian form,

$$r^+(\langle \alpha \rangle) = \tfrac{1}{2} r^+(\operatorname{Tr}_{K/K_0}(\langle \alpha \rangle))$$

since $\operatorname{Tr}_{K/K_0}(\langle \alpha \rangle)$ is the symmetric form $\langle 2\alpha, -2\delta\alpha \rangle$ over K_0.

There is also a signature defined when h is an Hermitian form over the Hamiltonian quaternions $(\mathbf{H}, ^*)$ over a real closed field $\mathbf{R}$. In this case $h \cong \langle \alpha_1, \ldots, \alpha_n \rangle$ with all $\alpha_i \in \mathbf{R}$, and $\operatorname{sgn}(h)$ is again defined as the number of positive α_i minus the number of negative α_i.

Another important property of formally real fields is that *if $(K, ^-)$ is definite and G is a finite group, then all simple components of KG are stable under the standard $(K, ^-)$-involution of KG.* This follows from the fact that G is an orthonormal basis of the Hermitian space $(KG, \operatorname{Tr}_{KG/K}(u\bar{v}))$; thus it is a positive definite space and so $\operatorname{Tr}_{KG/K}(u\bar{u}) > 0$ if $u \neq 0$ – in particular if u is in a simple component A of KG, then $\bar{u} \in A$ also since $u\bar{u} \neq 0$.

The following lemma will be useful later on:

Lemma 1.4.2 *Let $(K, ^-)$ be a field with involution $^- \neq \mathrm{id}$, and $K = K_0(\sqrt{\delta})$.*

(a) If $\mathbf{C}$ is an algebraic closure of K, then $\mathbf{C} \otimes_{K_0} K \cong \mathbf{C} \oplus \mathbf{C}$ via the map $(\alpha \otimes \lambda) \to (\alpha\lambda, \alpha\bar{\lambda})$, and the involution induced on $\mathbf{C} \oplus \mathbf{C}$ by $\mathrm{id} \otimes {}^-$ on $\mathbf{C} \otimes_{K_0} K$ is the interchange $\overleftrightarrow{(\beta_1, \beta_2)} = (\beta_2, \beta_1)$.

(b) Let $\mathbf{R}$ be a real closed field containing K_0 and P the restriction to K_0 of the ordering of $\mathbf{R}$. Let $\mathbf{C}$ be an algebraic closure $\mathbf{R}(i)$ containing K. Then

$$(\mathbf{R} \otimes_{K_0} K, \mathrm{id}_{\mathbf{R}} \otimes {}^-) \cong \begin{cases} (\mathbf{C}, ^*) & \textit{if } K/K_0 \textit{ is definite at } P, \\ (\mathbf{R} \oplus \mathbf{R}, \leftrightarrow) & \textit{if } K/K_0 \textit{ is indefinite at } P. \end{cases}$$

The isomorphism in (a) follows from Prop. 1.2.3 and Th. 1.2.15, p. 21. And it is easy to see that it is an isomorphism

$$(\mathbf{C} \otimes_{K_0} K, \mathrm{id} \otimes {}^-) \cong (\mathbf{C} \oplus \mathbf{C}, \leftrightarrow),$$

so (a) is proved.

If K/K_0 is definite at P, that is to say $\delta < 0$ at P where $K = K_0(\sqrt{\delta})$, $\mathbf{R}(\sqrt{\delta}) = \mathbf{C}$ and (b) follows easily in this case. If K/K_0 is indefinite at P, then $\delta > 0$ at P, $K \subset \mathbf{R}$ and

$$\mathbf{R} \otimes_{K_0} K \ \overset{\sim}{\to}\ \mathbf{R} \oplus \mathbf{R} \quad \text{via} \quad \rho \otimes \alpha \to (\rho\alpha, \rho\bar{\alpha}).$$

It is clear this is the isomorphism of involution algebras in (b). □

Proposition 1.4.1 *Suppose that K is a formally real algebraic number field (of finite degree over $\mathbb{Q}$) and that $\sigma_i : K \to \mathbb{R}$, $1 \le i \le r$, are the distinct imbeddings of K into the real numbers. Then the orderings on K are $P_1, \dots, P_r$ where $P_i = \sigma_i^{-1}\dot{\mathbb{R}}^2$ and they are distinct.*

Let $\mathbf{R}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{R}$. Suppose we show that it is a real closure of $\mathbb{Q}$ (for its unique ordering). Since $\sigma_i K \subset \mathbf{R}$, the σ_i are the distinct imbeddings $K \to \mathbf{R}$, so by pp. 115-116, [65], the distinct orderings of K are the $\sigma_i^{-1}\dot{\mathbf{R}}^2$; but $\sigma_i^{-1}\dot{\mathbf{R}}^2 = \sigma_i^{-1}\dot{\mathbb{R}}^2$ since $\mathbf{R} \cap \dot{\mathbb{R}}^2 = \dot{\mathbf{R}}^2$.

To show that $\mathbf{R}$ is a real closure of $\mathbb{Q}$, it suffices to show that $\mathbf{R}(i)$ is algebraically closed (Th. 1.4.4, p. 38).

Suppose $p(X) \in \mathbb{Q}[X]$ is monic of degree > 1. Factor it over $\mathbb{R}$:

$$p(X) = l_1 \dots l_r q_1 \dots q_s$$

where the l_i are monic linear polynomials and the q_i are monic irreducible quadratic polynomials. Since the roots of p are algebraic (over $\mathbb{Q}$), $p_i, q_j \in \mathbf{R}[X]$ for all i, j. Suppose $q_i = X^2 + \beta X + \gamma$. Its roots are $\frac{1}{2}(-\beta \pm \sqrt{\beta^2 - 4\gamma})$. Since $\beta^2 - 4\gamma < 0$, $\sqrt{\beta^2 - 4\gamma} = (\sqrt{4\gamma - \beta^2})i \in \mathbf{R}i$ since $\sqrt{4\gamma - \beta^2}$ is algebraic over $\mathbb{Q}$, and so $\mathbf{R}(i)$ is algebraically closed since it is an algebraic closure of $\mathbb{Q}$. □

Thus the orderings on a number field K are in canonical bijective correspondence with the real primes of K – which are the equivalence classes of the valuations $\alpha \to |\sigma_i \alpha|$ of K (where $|\ \cdot\ |$ is the absolute value on $\mathbb{R}$).

Corollary 1.4.2 *Suppose the ordering P_1 of the algebraic number field K_1 (of finite degree over $\mathbb{Q}$) can be extended to an ordering of the finite Galois extension K/K_1. Then the extensions of P_1 to K are the conjugates $\{\sigma P : \sigma \in \mathrm{Gal}(K/K_1)\}$ of any one of them.*

Let $\tau_1 : K_1 \to \mathbb{R}$ be an imbedding such that $P_1 = \tau_1^{-1}\dot{\mathbb{R}}^2$, let $\mathfrak{p}_1$ be the corresponding real prime – the equivalence class of the valuation $\alpha_1 \to |\tau_1(\alpha_1)|$ of K_1 – and let $\mathfrak{P}$ be a real prime of K lying over $\mathfrak{p}$. It is the equivalence class of a valuation $\alpha \to |\tau(\alpha)|$ of K given by an imbedding $\tau : K \to \mathbb{R}$ extending τ_1. By [53], Prop. 9.1, p. 167, the distinct primes of K lying over $\mathfrak{p}$ are the conjugates $\mathfrak{P}^\sigma$, the equivalence classes of the valuations $\alpha \to |\tau\sigma\alpha|$, $\sigma \in \mathrm{Gal}(K/K_1)$. Thus the extensions of P_1 to K are the conjugates

$$(\tau\sigma)^{-1}\dot{\mathbb{R}}^2 = \sigma^{-1}(\tau^{-1}\dot{\mathbb{R}}^2)$$

of the ordering $P = \tau^{-1}\dot{\mathbb{R}}^2$. □

Theorem 1.4.8 Frobenius' Theorem *If $\mathbf{R}$ is real closed, then up to isomorphism, the only finite dimensional division algebras over $\mathbf{R}$ are $\mathbf{R}, \mathbf{C} = \mathbf{R}(i)$, and the Hamiltonion quaternions $\mathbf{H} \cong (-1, -1)_{\mathbf{R}}$.*

The only finite extension fields of $\mathbf{R}$ are $\mathbf{R}$ itself and $\mathbf{C}$. The center of any division algebra finite dimensional over $\mathbf{R}$ must be one of these fields, and since there are no nontrivial finite dimensional division algebras over an algebraically closed field, any noncommutative division algebra over $\mathbf{R}$ must have center $\mathbf{R}$. Since the only proper finite extension field of $\mathbf{R}$ has degree 2, the maximal subfields of a proper division algebra have degree 2, so the division algebra has dimension 4 over $\mathbf{R}$ (cf. p. 12), hence is a quaternion algebra $(\alpha, \beta)_{\mathbf{R}}$ over $\mathbf{R}$ (cf. p. 16). This quaternion algebra splits if α or β is positive since the norm form is then isotropic, so both must be negative. Since positive elements of $\mathbf{R}$ are squares, the quaternion algebra is $\cong (-1,-1)_{\mathbf{R}}$, the Hamiltonian quaternion algebra $\mathbf{H}$. □

1.5 Bilinear and sesquilinear forms

This section consists of an outline of the algebraic theory of sesquilinear, bilinear, Hermitian, skew symmetric and symmetric forms, with few proofs. References are Chs. 1 and 2 in [39] and Chs. 1,2 and 7 in [65]. Later in Ch. 3 we shall give proofs for most of these matters in the more general setting of forms over a separable K-algebra with involution – such forms are necessary to deal with questions about orthogonal, symplectic and unitary representations over K.

1.5.1 Definitions and basic properties. Let D be a finite dimensional division algebra over the field K, with a $(K, {}^-)$-involution ${}^-$. (Keep in mind our blanket assumption that $\operatorname{char} K \neq 2$). Let V be a finite dimensional (left) vector space over D, say of dimension n, and let $V^* = \operatorname{Hom}_D(V, D)$ be its dual space. The canonical pairing $V \times V^* \to D$ is denoted by $\langle v, x \rangle$.

A *sesquilinear form* on V is a map

$$f : V \times V \to D$$

which is biadditive, linear in the first variable and semilinear with respect to ${}^-$ in the second. Thus f satisfies

$$\begin{aligned} f(u+u', v) &= f(u,v) + f(u',v), \\ f(u, v+v') &= f(u,v) + f(u,v'), \\ f(du, d'v) &= df(u,v)\bar{d}'. \end{aligned}$$

We usually write

$$f : V \times V \to (D, {}^-)$$

to indicate the dependence of f on the involution.

In this section, we write all mappings on the left including homomorphisms

$$\varphi : V \to W$$

from one *left* D-space to another – this accounts for the unorthodox relationship

$$\operatorname{mat}(\psi\varphi) = (\operatorname{mat}\varphi)(\operatorname{mat}\psi), \quad \text{i.e.} \quad \underline{\psi\varphi} = \underline{\varphi}\ \underline{\psi},$$

if $\psi : W \to U$ is another such homomorphism and $\operatorname{mat}\varphi = \underline{\varphi} = (\underline{\varphi}_{ij}) \in D^{n\times m}$, for example, is defined by $\varphi v_i = \sum_j \underline{\varphi}_{ij} w_j$ with respect to the bases $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, w_m\}$ of V and W respectively. This also means that if we use these bases to identify V and W with $D^{1\times n}$ and $D^{1\times m}$ respectively, then

$$\varphi v = v\underline{\varphi}.$$

If the involution ${}^-$ is the identity, then D is a field since $\overline{dd'} = \bar{d}'\bar{d}$ is $dd' = d'd$. In this case f is usually called a *bilinear form*.

Let $\varepsilon = \pm 1$. A sesquilinear form f which satisfies the symmetry condition

$$f(u,v) = \varepsilon\overline{f(v,u)} \quad \text{for all } u, v \in V,$$

will be called a *reflexive* form (over D or $(D, {}^-)$), or more precisely an ε-*reflexive* form. If the involution is known to be the identity, it is called an ε-*symmetric* bilinear form, or a *symmetric* bilinear form if $\varepsilon = 1$ and a *skew symmetric* bilinear form if $\varepsilon = -1$. If the involution is *not* the identity, it is called an *ε-Hermitian* form, or an *Hermitian* form if $\varepsilon = 1$ and a *skew Hermitian* form if $\varepsilon = -1$.

The map

$$f_r : V \to V^* \text{ given by } f_r(v) = f(\cdot, v)$$

is the *(right) adjoint* of the sesquilinear form f. Thus

$$\langle u, f_r(v)\rangle = f(u, v).$$

V^* is naturally a right vector space over D, and f_r satisfies

$$f_r(dv) = f_r(v)\bar{d} \quad \text{for all } d \in D \text{ and } v \in V.$$

Such a map, from a left D-space to a right D-space, is called a $(D, {}^-)$-*homomorphism*. Alternatively we can twist V^* into a *left* vector space $\overline{V^*}$ over D by defining a left D-action on V^*:

$$dx = x\bar{d}.$$

We often write $\bar{x}$ for x when we are considering it to be in $\overline{V^*}$; then this equation becomes

$$d\bar{x} = \overline{x\bar{d}} \quad \text{or} \quad \overline{xd} = \bar{d}\bar{x}.$$

Then the adjoint is a D-*linear* map

$$f_r : V \to \overline{V^*}.$$

The sesquilinear form f is *nonsingular* if its (right) adjoint is an isomorphism, and in this case (V, f) is called a *sesquilinear space* – or a *bilinear space* if ${}^-$ is known to be the identity (and D a field). We also say, loosely, that V is nonsingular if f is so. If f is ε-reflexive and nonsingular, the pair (V, f) is called a *reflexive space*, or an *ε-reflexive space*. Symmetric, skew symmetric, Hermitian and skew Hermitian spaces are similarly defined.

There is similarly a *left* adjoint

$$f_l : V \to \overline{V^*} \qquad \text{given by } f_l(v) = \overline{f(v, \cdot)},$$

that is to say,

$$\langle u, f_l(v)\rangle = \overline{f(v, u)}.$$

It is also a D-linear transformation.

The *discriminant matrix*[7] of (V, f) or f with respect to a basis $v_1, v_2, \ldots, v_n$ of V is the $n \times n$ matrix

$$\text{mat } f = \underline{f} = (f(v_i, v_j)) \in D^{n\times n}.$$

It is easy to see that f is symmetric or Hermitian if and only if $\underline{f}^{t-} = \underline{f}$, i.e. the matrix $\underline{f}$ is respectively symmetric or Hermitian, and is skew symmetric or skew Hermitian if and only if $\underline{f}^{t-} = -\underline{f}$, i.e. $\underline{f}$ is respectively skew symmetric or skew Hermitian. If we identify V with $D^{1\times n}$ using the basis, then

$$f(u, v) = u\underline{f}v^{t-}. \tag{1.33}$$

If $u_1, u_2, \ldots, u_n$ is another basis, related to the first by

$$u_i = \sum_k d_{ik} v_k,$$

[7] Also often called the *Gram matrix* of f.

then

$$f(u_i, u_j) = \sum_{k,\,l} d_{ik} f(v_k, v_l) \overline{d_{jl}}.$$

Thus the discriminant matrix of f with respect to the new basis is

$$\Delta \underline{f} \Delta^{t-}$$

where Δ is the matrix (d_{ij}) of the basis change. Assume now that D is a *separable* division algebra. Since $\mathrm{nrd}_{\mathrm{M}(n,D)/K} \Delta^{t-} = \overline{\mathrm{nrd}_{\mathrm{M}(n,D)/K} \Delta}$ by Lem. 1.3.7, p. 34, the *determinant* $\det f$ of f,

$$\det f = \mathrm{nrd}_{\mathrm{M}(n,D)/K} (\underline{f}),$$

is well defined up to a nonzero "norm" $\alpha\bar{\alpha}$ $(\alpha \in \mathrm{nrd}_{\mathrm{M}(n,D)/K} \mathbf{GL}(n, D) = \mathrm{nrd}_{D/K} \dot{D}$ – cf. (1.15), p. 14), and so can be considered to lie in $K/\mathrm{N}\dot{K} = \{0\} \cup \dot{K}/\mathrm{N}\dot{K}$ where $\mathrm{N}\dot{K}$ is the group of nonzero "norms" $\alpha\bar{\alpha}$ of K:

$$\mathrm{N}\dot{K} = \begin{cases} \dot{K}^2 & \text{if } {}^- = \mathrm{id} \text{ on } K, \\ \mathrm{N}_{K/K_0} \dot{K} & \text{otherwise.} \end{cases}$$

Note that $\det f \in K_0/\mathrm{N}_{K/K_0}\dot{K}$ if f is Hermitian.

If f is a nonsingular skew symmetric form, one can show that $\det f \in \dot{K}^2$, and so det is not a useful invariant in this case. On the other hand for each $n \geq 1$, there is a polynomial $\mathrm{Pf}_n \in \mathbb{Z}[X_{ij}; i, j = 1, \ldots, n, i \neq j]$ of degree n, called the *Pfaffian*, such that

$$\det(a_{ij}) = (\mathrm{Pf}_n(a_{ij}))^2$$

for any skew symmetric matrix $\in \mathrm{M}(2n, K)$. See Th. 3.27, p. 141, [2].

If $\det f = \alpha \mathrm{N}\dot{K}$, we often write $\det f = \alpha$. And if $\beta \in \alpha\mathrm{N}\dot{K}$, we also write $\det f = \beta =_{\mathrm{N}} \alpha$, or if $\mathrm{N}\dot{K} = \dot{K}^2$, $\det f = \beta =_2 \alpha$.

When $D = K$, we also define the *discriminant* of a symmetric or Hermitian form $h : V \times V \to (K, {}^-)$ to be $\operatorname{disc} h = (-1)^{n(n-1)/2} \det h$ where $n = \dim V$, and that of an even-dimensional skew Hermitian form to be $\operatorname{disc} h = \operatorname{disc} \sqrt{\delta} h \in \dot{K}_0/\mathrm{N}_{K/K_0}\dot{K}$; of course $\sqrt{\delta}h$ is an Hermitian form, and it depends on the choice of δ and $\sqrt{\delta}$ but $\operatorname{disc} \sqrt{\delta} h$ does not. The discriminant of an odd-dimensional skew Hermitian form is not defined.

Suppose that the sesquilinear form f is nonsingular, so $f(\cdot, v_1), \ldots, f(\cdot, v_n)$ is a basis of V^*. Let $v_1^*, \ldots, v_n^*$ be the dual basis of V^*. Then

$$f_r(v_i) = f(\cdot, v_i) = \sum_{j=1}^n v_j^* f(v_j, v_i) = \sum_{j=1}^n \overline{f(v_j, v_i)}\, v_j^*,$$

so the matrix of f_r with respect to the bases $\{v_i\}$ and $\{v_i^*\}$ is $(\mathrm{mat}\ f)^{t-}$. It follows that the determinant of f is $\neq 0$ if and only if f is nonsingular. Similarly

$$f_l(v_i) = \overline{f(v_i, \cdot)} = \sum_{j=1}^n f(v_i, v_j) v_j^*,$$

so the matrix of f_l is the discriminant matrix and f is nonsingular if and only if f_l is an isomorphism – in particular f_r is an isomorphism if and only if f_l is.

If U is a subspace of V and the form f is restricted to $U \times U$, we shall generally say it has been *restricted to* U. Such a subspace is called nonsingular if the restriction of f to it is nonsingular. Let

$$U^\perp = \{v \in V : f(U, v) = 0\},$$

the subspace of V *orthogonal to* U, which we also refer to as the *orthogonal complement* of U (in V). (Note that it is not necessarily the same as $\{v \in V : f(v, U) = 0\}$ unless f is reflexive.) Consider the sequence

$$0 \to U^\perp \xrightarrow{\text{incl}} V \xrightarrow{f_r} \overline{V^*} \xrightarrow{\text{restr}} \overline{U^*} \to 0$$

where the second map is inclusion and the fourth is restriction, $x \to x|_U$. The restriction is onto and if f is nonsingular, the kernel of the composite map $V \xrightarrow{f_r} \overline{V^*} \xrightarrow{\text{restr}} \overline{U^*}$ is $U^\perp$ and so

$$\dim U + \dim U^\perp = \dim \overline{U^*} + \dim U^\perp = \dim V.$$

If U also is nonsingular, $V = U \oplus U^\perp$ since then $U \cap U^\perp = 0$. In general if $f(U, W) = 0$ and $V = U \oplus W$, we shall write $V = U \perp W$ and say that V is the *orthogonal direct sum of* U and W. In this case U and W are both nonsingular if and only if V is. When this is so, $W = U^\perp$ and

$$\operatorname{mat} f = \begin{pmatrix} \operatorname{mat} g & 0 \\ * & \operatorname{mat} h \end{pmatrix}$$

where g is the restriction of f to U and h that to W. If we also have $f(W, U) = 0$, then of course

$$\operatorname{mat} f = \begin{pmatrix} \operatorname{mat} g & 0 \\ 0 & \operatorname{mat} h \end{pmatrix}.$$

This is in particular the case when $V = U \perp W$ and f is reflexive – which is almost always the case in the remainder of this book.

There is also an *external* orthogonal direct sum of sesquilinear spaces $(V_1, h_1) \perp (V_2, h_2) =$ (by definition) $(V_1 \perp V_2, h_1 \perp h_2)$ where $V_1 \perp V_2$ is the external direct sum $V_1 \oplus V_2$ and $(h_1 \perp h_2)(u_1 + u_2, v_1 + v_2) = h_1(u_1, v_1) + h_2(u_2, v_2)$. Here we have identified V_1 and V_2 with subspaces of $V_1 \oplus V_2$, so that $(v_1, v_2) = v_1 + v_2$. The external orthogonal direct sum is often denoted simply by $V_1 \perp V_2$ or $h_1 \perp h_2$. Obviously h_1 and h_2 do not have to be nonsingular in order for their external orthogonal direct sum to exist.

Let f be a nonsingular sesquilinear form on V. If $\varphi \in \operatorname{End}_D V$, its *adjoint* $\overline{\varphi} \in \operatorname{End}_D V$ is the transformation uniquely determined by

$$f(\varphi u, v) = f(u, \overline{\varphi} v) \quad \text{for all } u, v \in V. \tag{1.34}$$

The map $\varphi \to \overline{\varphi}$ is a $(K, {}^-)$-antiautomorphism of $\operatorname{End}_D V$, and is a $(K, {}^-)$-involution if f is reflexive. Using (1.33) and (1.34), one easily shows that the matrix $\underline{\overline{\varphi}}$ of the adjoint $\overline{\varphi}$ is given by

$$\begin{aligned} \underline{\overline{\varphi}} &= \underline{f}^{t-} \underline{\varphi}^{t-} (\underline{f}^{t-})^{-1} \\ &= \underline{f}\, \underline{\varphi}^{t-} \underline{f}^{-1} \ \text{ if } f \text{ is reflexive.} \end{aligned} \tag{1.35}$$

Exercises 1. Conversely, show that if $(D, {}^-)$ is a division algebra with involution and ${}^-$ is an involution on $\mathrm{M}(n, D)$ given by $\bar{a} = b a^{t-} b^{-1}$ for some $b \in \mathbf{GL}(n, D)$, it is the matrix version of the adjoint equation (1.35) with respect to a nonsingular reflexive form f on a vector space of dimension n over D.

2. If $(A, ^-)$ is a central simple algebra with involution, show that it is isomorphic to an involution algebra of the form $(\mathrm{M}(n, D), \, ^\sim \,)$ where D is a division algebra and $^\sim$ is the adjoint involution of some reflexive form. □

Proposition 1.5.1 *If $f : V \times V \to (K, ^-)$ is a nonsingular ε-reflexive form, the adjoint involution on $\mathrm{End}_K V$ is orthogonal if f is symmetric, symplectic if f is skew symmetric, and unitary if $^- \neq \mathrm{id}_K$.*

The case $^- \neq \mathrm{id}_K$ is trivial, so assume $^-$ is the identity on K. Then the proposition follows from (1.35) and Th. 1.3.6(b), p. 30, and the fact that transpose is an orthogonal involution. □

If f is reflexive but not skew symmetric, the space V has an *orthogonal basis*, i.e. a basis $v_1, \ldots, v_n$ such that $f(v_i, v_j) = 0$ if $i \neq j$. This means that the discriminant matrix mat f is diagonal with respect to this basis, with the diagonal entries $f(v_1, v_1) = d_1, \ldots, f(v_n, v_n) = d_n$. In this case we write $f = \langle d_1, d_2, \ldots, d_n \rangle$.

More generally, if $\underline{f}_1, \ldots, \underline{f}_k$ are square matrices over D, then the sesquilinear form whose discriminant matrix (with respect to some basis) is the matrix with the $\underline{f}_1, \ldots, \underline{f}_k$ as block diagonal matrices (and 0s elsewhere) is denoted by $\langle \underline{f}_1, \ldots, \underline{f}_k \rangle$.

If f is skew symmetric and nonsingular, then $f(v, v) = 0$ for all $v \in V$, and V is even dimensional and has a "symplectic" basis $v_1, \ldots, v_{2m}$ with the property that $f(v_{2i-1}, v_{2i}) = 1 = -f(v_{2i}, v_{2i-1})$ for all i and all other "inner products" $f(v_i, v_j)$ are $= 0$. In other words V is the orthogonal direct sum of m planes, each with discriminant matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{1.36}$$

Suppose again that $f : V \times V \to D$ is a sesquilinear form. A vector $v \in V$ is *isotropic* if $v \neq 0$ and $f(v, v) = 0$. V (or f) is called *isotropic* if it contains an isotropic vector, and is *totally isotropic* if f is identically 0.

A *hyperbolic plane* is a plane with an ε-reflexive form f with discriminant matrix

$$\mathrm{mat}\, f = \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix} \qquad (\varepsilon = \pm 1)$$

with respect to some basis. A *hyperbolic space* is, by definition, an orthogonal direct sum of one or more such planes (with the same ε). It is of course isotropic.

The following theorem is easily checked.

Theorem 1.5.1 *Let (V, f) be a plane with an ε-reflexive form f which is not skew symmetric. The following are equivalent.*

(a) V is a hyperbolic plane.

(b) $f = \langle d, -d \rangle$ where $d \in \dot{D}$ and $\bar{d} = \varepsilon d$.

(c) V is nonsingular and isotropic.

If $D = K$ and $\varepsilon = 1$, then these conditions are also equivalent to

(d) $\det f = -1$. □

Theorem 1.5.2 *Let (V, f) be a nonsingular ε-reflexive space, and let $U \subset V$ be a totally isotropic subspace of V with basis $u_1, \ldots, u_r$. Then there are vectors $w_1, \ldots, w_r$ in V such that if W is the space spanned by them,*

$$\operatorname{mat} f|_{U\oplus W} = \operatorname{diag}\left(\begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix} \right)$$

in the basis $u_1, w_1, u_2, w_2, \ldots, u_r, w_r$. □

A corollary is that a nonsingular alternating form has a symplectic basis, as stated earlier.

Let (V, f) be a sesquilinear space over $(K, {}^-)$, and $(L, {}^-)/(K, {}^-)$ an extension of fields with involution. Then there is a unique extension of f to a sesquilinear form f^L on the L-vector space $V^L = L \otimes_K V$ (which we assume contains V). This process is called "extension of the scalars". (The notation V_L and f_L is sometimes used, but we wish to reserve this for "restriction of scalars").

A little more generally, if $\varphi : (K, {}^-) \to (L, {}^-)$ is a homomorphism of fields with involution, then we can also "extend the scalars" to L. The resulting extension is a sesquilinear form

$$f^L : V^L \times V^L \to (L, {}^-)$$

on $V^L = L \otimes_K V$ (where K operates on L via $\alpha.\lambda = \varphi(\alpha)\lambda$, $\alpha \in K, \lambda \in L$), satisfying

$$f^L(\lambda \otimes u, \lambda' \otimes v) = \lambda\varphi(f(u, v))\overline{\lambda'} \qquad (\lambda, \lambda' \in L,\ u, v \in V). \tag{1.37}$$

Since a K-basis of V is also an L-basis of V^L, f and f^L have the same discriminant matrix and so f is nonsingular if and only if f^L is nonsingular. Also f is symmetric if and only if f^L is symmetric, and a similar statement holds when f is skew symmetric, Hermitian or skew Hermitian.

One can also extend the scalars when f is a sesquilinear form over a division algebra D; this process sometimes leads to a sesquilinear form over an algebra, and is discussed later (p. 110*ff*).

1.5.2 Isometries. Let (V, f) and (W, g) be sesquilinear forms over the division algebra $(D, {}^-)$ with involution. A *morphism* $\varphi : (W, g) \to (V, f)$ is a D-linear map $\varphi : W \to V$ such that $f(\varphi w, \varphi w') = g(w, w')$ for all $w, w' \in W$. It is necessarily injective if W is nonsingular, and is called an *isometry* if it is bijective. Two sesquilinear forms are *equivalent* if there is an isometry between them. In this case we write $(V, f) \cong (W, g), V \cong W$, or $f \cong g$, depending on the context.

One of the principal questions in the theory of sesquilinear spaces is the determination of invariants which characterize their equivalence classes. The nature of these invariants depends on whether the forms are Hermitian, symmetric, etc., and on the nature of the field K. The simplest invariants are the dimension of V and the determinant $\det f$.

The case of skew symmetric forms is trivial: since any nonsingular skew symmetric form has a symplectic basis, the dimension of a nonsingular skew symmetric form completely determines its equivalence class. The equivalence theory for other reflexive forms is much more complicated in general, and a summary of results for them is given in §1.5.7. The equivalence question for arbitrary sesquilinear spaces "reduces" to the reflexive case (cf. [57] and [61]), but we shall not need this theory.

The equivalence of reflexive forms over a field $(K, {}^-)$ with involution, which are not skew symmetric, can also be reduced to that of symmetric bilinear forms. First of all if h is skew Hermitian and $K = K_0(\sqrt{\delta})$, then $g = \sqrt{\delta}h$ is Hermitian. Furthermore any isometry between two skew Hermitian forms is also an isometry between the Hermitian forms associated to them in this way, and conversely. Thus when $K \neq K_0$, it suffices to consider the case of Hermitian forms. If h_1 and h_2 are Hermitian forms, they are equivalent if and only if their "trace forms" $h_i(u,v) + \overline{h_i(u,v)}$ are equivalent as symmetric bilinear forms over K_0. This is a theorem of Jacobson [30], and a proof is also given in Th. 10.1.1, p. 348, [65]. This also holds over a quaternion division algebra D with conjugation as involution, using the canonical trace of the quaternion algebra,

$$\mathrm{Tr}_{D/K}(\alpha + \beta i + \gamma j + \delta k) = \alpha,$$

or equivalently the reduced trace $\mathrm{trd}_{D/K}$ – see Th. 10.1.7, p. 352, *ibid.*

Exercises. 1. Show that if f and g are equivalent nonsingular reflexive forms over $(D, {}^-)$, then their adjoint involutions (on the algebras of endomorphisms of their vector spaces) are equivalent.

2. If ${}^-$ and ${}^\sim$ are symplectic involutions on $\mathrm{M}(2n, K)$, show that $(\mathrm{M}(2n, K), {}^-) \cong (\mathrm{M}(2n, K), {}^\sim)$. (Cf. the exercise on p. 46.) □

If we use bases for V and W over D to express $\varphi : (W, g) \to (V, f)$ as a matrix $\underline{\varphi}$ with entries in D, then the fact that φ is a morphism of sesquilinear spaces is expressed in terms of matrices by

$$\underline{g} = \underline{\varphi}\,\underline{f}\,\underline{\varphi}^{t-}.$$

The set of isometries $\varphi : V \to V$ of a sesquilinear space with itself is the *isometry group* of $f : V \times V \to (D, {}^-)$. It is denoted by $\mathbf{I}(V, f)$, $\mathbf{I}(V)$, or $\mathbf{I}(f)$, depending on the context. If f is known to be symmetric, it is called the *orthogonal group* and is denoted by $\mathbf{O}(V, f)$, etc. In the skew symmetric case, it is called the *symplectic group* and is denoted by $\mathbf{Sp}(V, f)$, and is the *unitary group* $\mathbf{U}(V, f)$ when f is ε-Hermitian.

The isometry group can also be viewed as the group of (invertible) matrices satisfying

$$\underline{\varphi}\,\underline{f}\,\underline{\varphi}^{t-} = \underline{f}. \tag{1.38}$$

Suppose that f is a nonsingular reflexive form over a field. Then (1.38) implies that $\det \underline{\varphi}\, \overline{\det \underline{\varphi}} = 1$, i.e. the norm of the determinant of an isometry is 1. In the skew symmetric case, it can be shown that $\det \underline{\varphi} = 1$. Suppose then that f is *not* skew symmetric. Then there is a vector $v \in V$ such that $f(v, v) \neq 0$ and we can split $V = Kv \perp W$. If $\lambda \in K$ has norm 1, the map $\varphi := \lambda(\mathrm{id}_{Kv}) \perp \mathrm{id}_W$ is an isometry with determinant λ. Thus if we define the "special" unitary group $\mathbf{SU}(V)$ respectively special orthogonal group $\mathbf{SO}(V)$ to be the subgroup of isometries of determinant 1, the sequences

$$1 \to \mathbf{SU}(V) \to \mathbf{U}(V) \to {}_N\dot{K} \to 1, \quad 1 \to \mathbf{SO}(V) \to \mathbf{O}(V) \to \pm 1 \to 1$$

are exact, where ${}_N\dot{K}$ is the subgroup of $\dot{K}$ of elements of norm 1.

One of the most important theorems for reflexive forms is

Theorem 1.5.3 Witt's Theorem. *Let $f : V \times V \to (D, {}^-)$ be a nonsingular reflexive form over $(D, {}^-)$, and suppose that $V = U_1 \perp W_1 = U_2 \perp W_2$ are splittings of V with $U_1 \cong U_2$. Then $W_1 \cong W_2$.* □

More generally, if U_1 and U_2 are equivalent subspaces of V which are not necessarily nonsingular, then $U_1^\perp \cong U_2^\perp$ (if V is nonsingular). And if $\varphi : (U, f|_{U\times U}) \to (V, f)$ is an injective morphism, it can be extended to an isometry of V. (This is proved later in a more general setting – see p. 100).

1.5.3 Witt rings. It follows from Theorem 1.5.2 (p. 48) that any ε-reflexive space V over $(D, {}^-)$ has a "Witt decomposition"

$$V = H \perp W$$

where H is hyperbolic and W is *anisotropic*, that is to say, W contains no isotropic vectors. By Witt's theorem, H and W are both determined up to an isometry. W is called the *anisotropic kernel* of V. The equivalence classes of anisotropic forms $[W]$ can be made into an associative commutative monoid by defining $[W_1]+[W_2] = [W_3]$ where $W_1 \perp W_2 = H \perp W_3$ is a Witt decomposition. This monoid can be imbedded in a group in which every element is of the form $[W] - [W']$ (cf. §1.6); it is called the *Witt group* and is denoted by $\mathrm{W}_\varepsilon(D)$, or more precisely by $\mathrm{W}_\varepsilon(D, {}^-)$. Of course since every nonsingular skew symmetric form is a sum of hyperbolic forms, the Witt group $\mathrm{W}_{-1}(K, \mathrm{id}_K)$ is trivial, so we ignore it in the rest of this discussion.

Since $\langle \alpha, -\alpha \rangle$ (where $\bar{\alpha} = \varepsilon\alpha \in \dot{D}$) is hyperbolic and hence $= 0$ in $\mathrm{W}_\varepsilon(D)$,

$$[-\alpha] = -[\alpha]$$

where we have written $[\alpha]$ for $[\langle \alpha \rangle]$.

In the case of symmetric forms or Hermitian forms over the field K, $\mathrm{W}_1(K) = \mathrm{W}_1(K, {}^-)$ is also a ring. Namely we can define the product $(V \otimes W, fg)$ of 2 forms (V, f) and (W, g) where

$$(fg)(v_1 \otimes w_1, v_2 \otimes w_2) = f(v_1, v_2)g(w_1, w_2), \tag{1.39}$$

which in terms of diagonalizations is

$$\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle \langle \beta_1, \beta_2, \ldots, \beta_m \rangle = \langle \alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_n\beta_m \rangle. \tag{1.40}$$

In general, the discriminant matrix of the product fg is the tensor product $\underline{f} \otimes \underline{g}$ of discriminant matrices (p. 17, [39]).

The product of two general sesquilinear forms f and g over $(K, {}^-)$ can also be defined by (1.39), and again has discriminant matrix $\underline{f} \otimes \underline{g}$ – if the forms happen to be ε-reflexive and δ-reflexive respectively, then the product fg is $\varepsilon\delta$-reflexive.

Since the product is distributive and the product of a hyperbolic space and an arbitrary nonsingular space is hyperbolic, $\mathrm{W}_1(K, {}^-)$ inherits a multiplication which makes it into a ring, the *Witt ring* of symmetric bilinear or Hermitian forms over $(K, {}^-)$. In fact multiplication can be extended to the "graded Witt ring"

$$\mathrm{W}(K, {}^-) := \mathrm{W}_1(K, {}^-) \oplus \mathrm{W}_{-1}(K, {}^-)$$

which is a $\mathbb{Z}/2$-graded ring, although as pointed out above, $\mathrm{W}_{-1}(K, \mathrm{id}\,) = 0$.

The product of forms is considered in greater generality in Ch. 3.

The Witt group $\mathrm{W}_\varepsilon(K, {}^-)$ can also be defined in another way via the Grothendieck group – this is discussed in Ch. 3 in the more general context of forms over an involution algebra. One begins with the monoid of equivalence classes $[h]$ of nonsingular ε-reflexive forms, which is imbedded in the corresponding Grothendieck group $\hat{\mathrm{W}}_\varepsilon(K,{}^-)$ – the "*Witt-Grothendieck group*" – whose elements are the differences $[h_1]-[h_2]$ (cf. §1.6). Then the Witt group $\mathrm{W}_\varepsilon(K,{}^-)$ is the quotient $\hat{\mathrm{W}}_\varepsilon(K,{}^-)/\mathbb{Z}[H]$ where H is an ε-reflexive hyperbolic plane.

In fact $\hat{\mathrm{W}}(K,{}^-) := \hat{\mathrm{W}}_1(K,{}^-) \oplus \hat{W}_{-1}(K,{}^-)$ is also a graded ring, and the subgroup generated by 1-reflexive and -1-reflexive hyperbolic forms is a graded ideal $\hat{\mathrm{H}}(K,{}^-)$ such that $\hat{\mathrm{W}}(K,{}^-)/\hat{\mathrm{H}}(K,{}^-) \cong \mathrm{W}(K,{}^-)$.

Now consider the Witt group $\mathrm{W}_1(K) = \mathrm{W}_1(K,{}^-)$ of symmetric or Hermitian forms. The dimension gives a homomorphism $\dim : \hat{\mathrm{W}}_1(K) \to \mathbb{Z}$ whose kernel is denoted by $\hat{I}$. Thus $\hat{\mathrm{W}}_1/\hat{I} \cong \mathbb{Z}$, and $\hat{I}$ is generated, as an Abelian group, by the differences of (equivalence classes of) unary (one dimensional) forms. Since $\hat{I} \cap \mathbb{Z}[H] = 0$, $\hat{I}$ is isomorphic to its image $I \subset \mathrm{W}_1(K)$, the *fundamental ideal* of $\mathrm{W}_1(K)$, consisting of the classes of all even dimensional forms. The kernel of the composite homomorphism $\hat{\mathrm{W}}_1(K) \to \mathbb{Z} \to \mathbb{Z}/2$ contains the classes of all even dimensional forms, hence the homomorphism factors through $\mathrm{W}_1(K)$, so we get a (surjective) homomorphism "dimension mod 2"

$$\dim_{/2} : \mathrm{W}_1(K) \to \mathbb{Z}/2$$

with kernel I which assigns to the Witt class $[h]$ the parity of its dimension, i.e. $\dim_{/2}[h] = \dim h + 2\mathbb{Z}$. In particular,

$$\mathrm{W}_1(K)/I \cong \mathbb{Z}/2.$$

Recall that the discriminant of h is

$$\operatorname{disc} h = (-1)^{\frac{1}{2}n(n-1)} \det h \in \dot{K}_0/\mathrm{N}\dot{K}$$

(p. 45) where $n = \dim h$ ($= \dim V$ if V is the space of h), and that $\mathrm{N}\dot{K} = \dot{K}^2$ if ${}^-$ is the identity on K, $= \mathrm{N}_{K/K_0}\dot{K}$ otherwise. The discriminant is well-defined on Witt classes, in contrast to the determinant, so we can consider it to be a map on $\mathrm{W}_1(K)$. Consider the map

$$(\mathrm{disc}, \dim_{/2}) : \mathrm{W}_1(K) \to \dot{K}_0/\mathrm{N}\dot{K} \times \mathbb{Z}/2. \tag{1.41}$$

If we define multiplication on the (set) product $\dot{K}_0/\mathrm{N}\dot{K} \times \mathbb{Z}/2$ by

$$(\alpha\mathrm{N}\dot{K}, i)(\beta\mathrm{N}\dot{K}, j) = ((-1)^{ij}\alpha\beta\mathrm{N}\dot{K}, i+j),$$

then $\dot{K}_0/\mathrm{N}\dot{K} \times \mathbb{Z}/2$ is a group, the *central extension of* $\mathbb{Z}/2$ *by* $\dot{K}_0/\mathrm{N}\dot{K}$ *with cocycle* $\mathrm{z}(i,j) = (-1)^{ij} \in \mathrm{Z}^2(\mathbb{Z}/2, \dot{K}_0)$,[8] which we denote by $\dot{K}_0/\mathrm{N}\dot{K} \times_{\mathrm{z}} \mathbb{Z}/2$. Moreover (1.41) is then an epimorphism with kernel I^2 and

$$\mathrm{W}_1(K)/I^2 \cong \dot{K}_0/\mathrm{N}\dot{K} \times_{\mathrm{z}} \mathbb{Z}/2, \quad I/I^2 \cong \dot{K}_0/\mathrm{N}\dot{K} \tag{1.42}$$

– cf. Prop. 2.1 and Cor. 2.2, pp. 31,32, [39] – it is proved there only for symmetric bilinear forms but the proof applies, *mutatis mutandis*, to the Hermitian case as well.

The Witt ring can be considered as a (covariant) functor W_1 from the category of involution fields of characteristic $\neq 2$ to the category of commutative rings since a homomorphism $(K,{}^-) \to (L,{}^-)$ gives rise, by scalar extension, to a ring homomorphism $\mathrm{W}_1(K,{}^-) \to \mathrm{W}_1(L,{}^-)$.

[8] where $\mathbb{Z}/2$ operates trivially on $\dot{K}_0$.

1.5.4 K real closed or algebraically closed.

Theorem 1.5.4 *If K is an algebraically closed field $\mathbf{C}$, two nonsingular symmetric bilinear forms are equivalent if and only if they have the same dimension. Furthermore*

$$\dim : \hat{\mathrm{W}}_1(\mathbf{C}, \mathrm{id}) \to \mathbb{Z} \quad \textit{and} \quad \dim_{/2} : \mathrm{W}_1(\mathbf{C}, \mathrm{id}) \to \mathbb{Z}/2$$

are both ring isomorphisms. □

Let $n\langle\alpha\rangle$ denote the n-fold sum $\langle\alpha\rangle \perp \langle\alpha\rangle \perp \cdots \perp \langle\alpha\rangle$.

Theorem 1.5.5 *Let $(\mathbf{C}, {}^*)$ be an algebraically closed field with an involution ${}^* \neq \mathrm{id}$.*

(a) The subfield of $\mathbf{C}$ of elements fixed by * is a real closed field $\mathbf{R}$.
(b) Up to equivalence, there are exactly two anisotropic symmetric forms over $(\mathbf{R}, \mathrm{id})$ or Hermitian forms over $(\mathbf{C}, {}^*)$ of dimension n, namely $n\langle 1\rangle$ and $n\langle -1\rangle$.
(c) $\mathrm{W}_1(\mathbf{R}, \mathrm{id}) \cong \mathrm{W}_1(\mathbf{C}, {}^*) \cong \mathbb{Z}$ (as commutative rings) via the signature map.
(d) (Sylvester's Law of Inertia) *Two nonsingular symmetric forms over $(\mathbf{R}, \mathrm{id})$ or Hermitian forms over $(\mathbf{C}, {}^*)$ are equivalent if and only if they have the same dimension and the same signature.*
(e) The identity of the Witt-Grothendieck ring is $\langle 1\rangle$, and if we identify $\mathbb{Z}\langle 1\rangle$ with $\mathbb{Z}$, then $\hat{\mathrm{W}}_1(K) = \mathbb{Z}[\langle -1\rangle]$ as a ring (note that $\langle -1\rangle^2 = \langle 1\rangle = 1$) and is $\cong \mathbb{Z} \oplus \mathbb{Z}$ as a group.

The subfield of $\mathbf{C}$ of elements fixed by * is a real closed field $\mathbf{R}$ by Th. 1.4.5 (p. 38).

Any nonsingular symmetric or Hermitian form is of the form $h = \langle \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n\rangle$ where for each i, $\varepsilon_i = \pm 1$, and the difference between the number of $1s$ and $-1s$ is the signature $\mathrm{sgn}(h) = r^+(h) - r^-(h)$ of h. It is additive and is $= 0$ on any hyperbolic space, so it induces a homomorphism $\mathrm{sgn} : \mathrm{W}_1(K) \to \mathbb{Z}$. The rest of the theorem follows without difficulty. □

Of course this theorem applies to an arbitrary real closed field $\mathbf{R}$ since $(\mathbf{C} : \mathbf{R}) = 2$ where $\mathbf{C} = \mathbf{R}(i)$.

We mention also *Pfister's Local-Global Principle* for symmetric bilinear forms (Th. 3.6.2, [65]): *The kernel of the canonical map*

$$\mathrm{W}_1(K) \to \prod_P \mathrm{W}_1(K_P)$$

is the torsion subgroup of $\mathrm{W}_1(K)$ *and is a 2-primary Abelian group.* Here P runs over the orderings of K, and K_P is a real closure of K for P. In particular if K is *not* formally real – for example if the characteristic of K is > 0 – the Witt group itself is a 2-primary torsion Abelian group.

1.5.5 Local and global fields. References for this section are [54], §12 and §13 of Ch. 2 and Ch. 5 in [65], as well as Ch. VI, [39].

For the moment, K continues to be an arbitrary field of characteristic $\neq 2$.

Let (V, b) be a symmetric space. If $\langle\alpha_1, \alpha_2, \ldots, \alpha_n\rangle$ is any diagonalization of b, the *Hasse algebra* of b is defined to be the tensor product of quaternion algebras

$$\mathrm{S}(b) = \underset{i<j}{\otimes}(\alpha_i, \alpha_j)_K.$$

It is independent of the chosen diagonalization (up to isomorphism), and is a central simple algebra since it is the tensor product of central simple (quaternion) algebras (cf. Th. (1.2.9), p. 9). Its Brauer class (cf. §1.2)

$$\mathrm{s}(b) = [\mathrm{S}(b)] \in \mathrm{Br}_2(K)$$

is called the *Hasse invariant* of b. Here $\mathrm{Br}_2(K)$ denotes the group of Brauer classes of order 1 or 2.

We will usually denote the Brauer class $[(\alpha, \beta)_K]$ by the same symbol $(\alpha, \beta)_K$ as the quaternion algebra itself – or even by (α, β) if the base field is obvious. It should be clear from the context which is meant. If it is necessary to make the field K explicit, we write s_K instead of s.

The quaternion Brauer classes satisfy the following identities (cf. [54], pp. 146, 147):

1. $(\alpha, \beta) = 1$ if and only if the algebra (α, β) is not a division algebra,
if and only if the "norm form" $xx^* = x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2$ is isotropic,
if and only if $\alpha \in \mathrm{N}_{K(\sqrt{\beta})/K}$.
2. $(\alpha, \beta) = (\beta, \alpha)$.
3. $(\alpha^2, \beta) = 1 = (\alpha, -\alpha) = (\alpha, 1 - \alpha)$.
4. $(\alpha, \alpha\beta) = (\alpha, -\beta)$.
5. $(\alpha, \beta)(\alpha, \gamma) = (\alpha, \beta\gamma), \qquad (\alpha, \beta)(\gamma, \beta) = (\alpha\gamma, \beta)$.
6. If L/K is a finite extension of local fields, $\alpha \in \dot{K}$ and $\lambda \in \dot{L}$, then

$$(\alpha, \lambda)_L = (\alpha, \mathrm{N}_{L/K}\lambda)_K.$$

See p. 102, [37] for the last property.

The following lemma follows easily (and tediously!) from the definition of s and the foregoing properties of the Brauer classes $(\alpha, \beta)_K$.

Lemma 1.5.1 *Let b be a nonsingular symmetric form of dimension n over K.*

(a) If $\alpha \in \dot{K}$,

$$\mathrm{s}(\alpha b) = \mathrm{s}(b)(\alpha, -1)_K^{n(n-1)/2}(\alpha, \det b)_K^{n-1}.$$

(b) If $b_1, \ldots, b_r$ are nonsingular symmetric forms over K,

$$\mathrm{s}(b_1 \perp \ldots \perp b_r) = \prod_i \mathrm{s}(b_i) \prod_{i<j}(\det b_i, \det b_j)_K.$$

(c) If $\alpha_1, \ldots, \alpha_m \in \dot{K}$,

$$\begin{aligned}&\mathrm{s}(\langle\det\alpha_1 b, \ldots, \det\alpha_m b\rangle)\\ &\quad = \mathrm{s}(\langle\alpha_1^n, \ldots, \alpha_m^n\rangle)(\det b, -1)_K^{m(m-1)/2}(\det b, \alpha_1\cdots\alpha_m)_K^{n(m-1)}.\end{aligned}$$

(d) *Let f be another nonsingular symmetric form, say of rank m. Then*

$$\begin{aligned} &\mathrm{s}(b \otimes f) \\ &= \quad \mathrm{s}(b)^m \mathrm{s}(f)^n (\det b, -1)_K^{m(m-1)/2} (\det b, \det f)_K^{mn-1} (\det f, -1)_K^{n(n-1)/2}. \end{aligned}$$

(e) *If b is hyperbolic of dimension $n = 2k$, then*

$$\mathrm{s}(b) = (-1, -1)_K^{k(k-1)/2}.$$

□

Theorem 1.5.6 *Let (V, b) and (V', b') be symmetric spaces over K.*

(a) *If they have dimension ≤ 3, they are equivalent if and only if*

$$\dim b = \dim b', \quad \det b = \det b', \quad \mathrm{s}(b) = \mathrm{s}(b'). \tag{1.43}$$

(b) *If V and V' have dimension 4 and (1.43) holds, the two forms are equivalent to scalar multiples of each other, i.e. $b' \cong \alpha b$ for some $\alpha \in \dot{K}$.*

(c) *If every symmetric space over K of dimension ≥ 5 is isotropic, two symmetric spaces V and V' (of any dimension) are equivalent if and only if (1.43) holds.*

In Scharlau's book [65], (a) is 13.5, p. 86, (b) is 14.1, p. 88, and (c) is 14.5, p. 91. □

Every symmetric space of dimension ≥ 5 over a local field is isotropic, and so by (c), we get

Theorem 1.5.7 *Two symmetric spaces over a local field are equivalent if and only if (1.43) holds.* □

In the case of a local field K, $\mathrm{Br}_2(K)$ is the group of order 2 (cf. p. 17), and we usually denote its elements by ± 1; in particular the Hasse invariant $\mathrm{s}(b) = \pm 1$.

There are two variations on the theme of the Hasse invariant. The first is usually called the *Witt invariant* $\mathrm{c}(b)$ – cf. p. 119, [39]) – and arises in a natural way from the theory of Clifford algebras (cf. p. 259). It is defined by

$$\begin{array}{rcll} \mathrm{c}(b) & = & \mathrm{s}(b) & \text{if } n \equiv 1, 2 \bmod 8 \\ \mathrm{c}(b) & = & \mathrm{s}(b)(-1, -\det b)_K & \text{if } n \equiv 3, 4 \bmod 8 \\ \mathrm{c}(b) & = & \mathrm{s}(b)(-1, -1)_K & \text{if } n \equiv 5, 6 \bmod 8 \\ \mathrm{c}(b) & = & \mathrm{s}(b)(-1, \det b)_K & \text{if } n \equiv 7, 8 \bmod 8. \end{array}$$

Unlike the Hasse invariant, it is well-defined on Witt classes, and in fact provides an isomorphism

$$I^2/I^3 \to \mathrm{Br}_2(K)$$

for an arbitrary field K (of characteristic $\neq 2$ of course). It is characterized by the fact that it is well-defined on the Witt group $\mathrm{W}_1(K)$ and coincides with the Hasse invariant when $n \equiv 1$ or $2 \bmod 8$.

The other variant of the Hasse invariant is the *Hasse-Witt invariant* which we shall denote by $\mathrm{w}(b)$ (or $\mathrm{w}_K(b)$ if the field K is not clear from the context). It also takes its values in $\mathrm{Br}_2(K)$, and can be defined by the property that it too is well-defined on the Witt group and coincides with the Hasse invariant when $n \equiv 0$ or 1 mod 8. One can show that this means that

$$\begin{array}{rcll} \mathrm{w}(b) & = & \mathrm{s}(b) & \text{if } n \equiv 0,1 \bmod 8 \\ \mathrm{w}(b) & = & \mathrm{s}(b)(-1,-\det\, b)_K & \text{if } n \equiv 2,3 \bmod 8 \\ \mathrm{w}(b) & = & \mathrm{s}(b)(-1,-1)_K & \text{if } n \equiv 4,5 \bmod 8 \\ \mathrm{w}(b) & = & \mathrm{s}(b)(-1,\det\, b)_K & \text{if } n \equiv 6,7 \bmod 8. \end{array}$$

It is clear that Ths. 1.5.6 and 1.5.7 continue to hold if s is replaced by c or w.

Exercise. Show that the Witt and Hasse-Witt invariants are well-defined on Witt classes, and that they are characterized by this fact and the fact that they agree with the Hasse invariant when $n \equiv 1,2$ mod 8 respectively $n \equiv 0,1$ mod 8. □

Another result needed later is:

Lemma 1.5.2 *If b is a nonsingular symmetric form of rank n over K and $\alpha \in \dot{K}$, then*

$$\mathrm{w}(\alpha b) = \mathrm{w}(b)(\alpha, \operatorname{disc} b)_K^{n+1}.$$

For example, if $n \equiv 3$ mod 8,

$$\begin{array}{rcll} \mathrm{w}(\alpha b) & = & \mathrm{s}(\alpha b)(-1,-\det \alpha b)_K & \\ & = & \mathrm{s}(b)(\alpha,-1)_K^{(n-1)/2}(-1,-\alpha \det b)_K & \text{by Lem. 1.5.1(a) since } n \text{ is odd} \\ & = & \mathrm{s}(b)(-1,-\det b)_K(\alpha,-1)_K^{(n+1)/2} = \mathrm{w}(b). & \end{array}$$

The other 7 cases can be proved in a similar fashion, and are left to the reader. □

Theorem 1.5.8 The Hasse-Minkowski Theorem. *Two symmetric spaces over a global field K of characteristic $\neq 2$ are equivalent if and only if for each prime $\mathfrak{p}$ of K, their completions ("scalar extensions") over $K_{\mathfrak{p}}$ are equivalent .* □

Furthermore one need only check the real primes and those nonArchimedean primes $\mathfrak{p}$ at which 2 or the discriminant of the forms is not a unit.

Using Jacobson's theorem (cf. p. 49), one can use Ths. 1.5.5, 1.5.7 and 1.5.8 to solve the Hermitian case as well:

Theorem 1.5.9 *Suppose that h and g are nonsingular Hermitian forms over $(K, ^-)$, $^- \neq \mathrm{id}$.*

(a) If K_0 is a real closed field, h and g are equivalent if and only if they have the same dimension and signature.

(b) If K is a local field, h and g are equivalent if and only if they have the same dimension and discriminant.

(c) If K is a global field, $K = K_0(\sqrt{\delta})$, then h and g are equivalent if and only if they have the same dimension, discriminant and, at each real prime at which $\delta < 0$, the same signature. □

The next three lemmas are needed in Ch. 5.

Lemma 1.5.3 *The quadratic form $q = \langle \alpha, \beta, -\alpha\beta \rangle$, $\alpha\beta \neq 0$, over the global field K represents an infinite number of square classes of K.*

The quadratic form $\langle 1\rangle \perp -q$ is the norm form of the quaternion algebra $D = (\alpha, \beta)_K$. If D is split, it is isomorphic to $(\gamma, 1)_K$ for any $\gamma \in \dot{K}$ (p. 16, (b)) and since the norm form of this algebra is $\langle 1, -\gamma, -1, \gamma\rangle$, $q \cong \langle \gamma, 1, -\gamma\rangle$ and so represents γ.

Therefore we may assume that D is *not* split over K. Let S consist of the (positive even number of) primes of K at which $D_{\mathfrak{p}}$ is not split (cf. Ex. 5, p. 18). If $\mathfrak{p} \notin S$, $q_{\mathfrak{p}}$ represents all elements of $K_{\mathfrak{p}}$ by the argument used above for K.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be primes not in S. For each i, choose a nonsquare γ_i of $K_{\mathfrak{p}_i}$. Let M be an arbitrary subset of $\mathrm{N} = \{1, \ldots, n\}$. By the approximation theorem for valuations (p. 18), we can find $\gamma \in \dot{K}$ which is arbitrarily close to γ_i at $\mathfrak{p}_i$ for each $i \in \mathrm{M}$, arbitrarily close to 1 for each $i \in \mathrm{N} \setminus \mathrm{M}$, and arbitrarily close to α at each prime of S. If the approximation is close enough,

$$\gamma \in \begin{cases} \gamma_i \dot{K}^2_{\mathfrak{p}_i} & \text{for all } i \in \mathrm{M}, \\ \dot{K}^2_{\mathfrak{p}_i} & \text{for all } i \in \mathrm{N} \setminus \mathrm{M}, \\ \alpha \dot{K}^2_{\mathfrak{p}} & \text{for each prime in } S, \end{cases}$$

by an obvious argument for Archimedean primes, and by the Local Square Theorem in the case of finite primes. It follows that γ is represented by q at *every* prime $\mathfrak{p}$ of K, and so also over K by the Hasse Principle for "representations" of one quadratic form by another (p. 189, [54]).

There are 2^n choices for M, leading to 2^n distinct square classes of K. Since n is arbitrary, the lemma follows. □

Lemma 1.5.4 *If K is a global field and L/K is a quadratic extension, then $[\dot{K} : \mathrm{N}_{L/K}\dot{L}]$ is infinite.*

We note first that the norms – and therefore also the non-norms – in a quadratic extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ of local fields form an open subset of $K_{\mathfrak{p}}$. This follows easily from the Local Square Theorem according to which an element of $K_{\mathfrak{p}}$ sufficiently close to 1 is a square in $K_{\mathfrak{p}}$ – and hence a norm in $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ be a sequence of distinct primes of K which do not split in L/K (cf. 3.7, p. 378, [53]). Let N be a positive integer, and for each $i, 1 \leq i \leq N$, choose a nonnorm $\alpha_i \in \dot{K}_{\mathfrak{p}_i}$. Apply the approximation theorem (p. 18) to find $\beta_i \in \dot{K}$ which is close to α_i at $\mathfrak{p}_i$ and close to 1 at the other $\mathfrak{p}_j$. If the approximations are good enough, for each $i \neq j$, $\beta_i \beta_j^{-1}$ is not a norm in $K_{\mathfrak{p}_i}$ (nor in $K_{\mathfrak{p}_j}$ for that matter) and hence is certainly not a norm in the extension L/K. Thus $\beta_1, \ldots, \beta_N$ are in distinct cosets of $\dot{K}/\mathrm{N}_{L/K}\dot{L}$ and the lemma follows. □

Let L/K be a finite Abelian extension of local fields, $\mathcal{G} = \mathrm{Gal}(L/K)$ its Galois group, and $\bar{\mathrm{N}} : \dot{L}/\dot{L}^2 \to \dot{K}/\dot{K}^2$ the homomorphism induced by $\mathrm{N}_{L/K}$. The image of $\bar{\mathrm{N}}$ is $(\mathrm{N}_{L/K}\dot{L})\dot{K}^2/\dot{K}^2$.

Lemma 1.5.5 $|\ker \bar{\mathrm{N}}| = \frac{[\dot{L}:\dot{L}^2]}{|\mathrm{im}\,\bar{\mathrm{N}}|} = \frac{[\dot{L}:\dot{L}^2]}{[\dot{K}:\dot{K}^2]}[\mathcal{G} : \mathcal{G}^2]$, *which is* $= [\mathcal{G} : \mathcal{G}^2]$ *if K is nondyadic since* $[\dot{K} : \dot{K}^2] = 4$ *for any nondyadic field ((p. 217,* [65]*).*

By local class field theory (p. 18), there is a (canonical) isomorphism $\dot{K}/\mathrm{N}_{L/K}\dot{L} \cong \mathcal{G}$, so there is an isomorphism between their subgroups generated by squares:

$\dot{K}^2 \mathrm{N}_{L/K}\dot{L}/\mathrm{N}_{L/K}\dot{L} \cong \mathcal{G}^2$. Thus

$$\begin{aligned} |\mathrm{im}\,\bar{N}| &= [(\mathrm{N}_{L/K}\dot{L})\dot{K}^2 : \dot{K}^2] = \frac{[\dot{K} : \dot{K}^2]}{[\dot{K} : (\mathrm{N}_{L/K}\dot{L})\dot{K}^2]} \\ &= \frac{[\dot{K} : \dot{K}^2][(\mathrm{N}_{L/K}\dot{L})\dot{K}^2 : \mathrm{N}_{L/K}\dot{L}]}{[\dot{K} : \mathrm{N}_{L/K}\dot{L}]} \\ &= \frac{[\dot{K} : \dot{K}^2]|\mathcal{G}^2|}{|\mathcal{G}|} = \frac{[\dot{K} : \dot{K}^2]}{[\mathcal{G} : \mathcal{G}^2]}. \end{aligned}$$

□

1.5.6 Trace forms over local fields. If $(L, ^-)/(K, ^-)$ is a finite extension of fields with involution, an (involution) trace (cf. p. 35)

$$\mathrm{t} : (L, ^-) \to (K, ^-)$$

is simply a nonzero K-linear map $\mathrm{t} : L \to K$ which commutes with the involutions,

$$\mathrm{t}(\bar{\alpha}) = \overline{\mathrm{t}(\alpha)} \text{ for all } \alpha \in L. \tag{1.44}$$

For example if L/K is separable, the field trace $\mathrm{Tr}_{L/K}$ is such a trace (Lem. 1.3.5, p. 33). If h is a nonsingular Hermitian form over $(L, ^-)$, it is easy to see that

$$(\mathrm{t}h)(u, v) = \mathrm{t}(h(u, v)) : V \times V \to (K, ^-) \tag{1.45}$$

is a nonsingular symmetric or Hermitian form over $(K, ^-)$. It is called the *transfer* of h with respect to (or via) t.

Transfers are of central importance in representation theory and will be studied systematically later in §3.2.3. Here we wish to deal with a special case which is important for representations over local and global fields (cf. Ch. 5).

The next lemma uses the notion of "field discriminant". If L/K is a finite separable extension, the usual notion of field discriminant is the determinant of the matrix $(\mathrm{Tr}_{L/K}\,\lambda_i\lambda_j)$ where $\lambda_1, \ldots, \lambda_l$ is a basis of L/K – this is the same thing as the determinant of the transfer of the form $\langle 1 \rangle$ over L to K – but we shall call this the *determinant of the extension* L/K, and denote it by $\det L/K$, since this is more consistent with the terminology of reflexive forms. We define the *discriminant of* L/K to be

$$\mathrm{disc}\, L/K = \mathrm{disc}\,(\mathrm{Tr}_{L/K}\,\langle 1 \rangle) = (-1)^{l(l-1)/2} \det L/K$$

where $l = (L : K)$.

Lemma 1.5.6 *Let $(L, ^-)/(K, ^-)$ be a finite extension of involution fields of the same kind*[9] *such that L/K is separable. Suppose that $h : V \times V \to (L, ^-)$ is either a symmetric bilinear form or an Hermitian or skew Hermitian form of rank* $\dim_L V = n$. *Then* $\det(L/K) \in K_0$, *the transfer* $\mathrm{Tr}_{L/K}h : V \times V \to (K, ^-)$ *has determinant*

$$\det \mathrm{Tr}_{L/K}h = (\det L/K)^n \mathrm{N}_{L/K}(\det h),$$

and, if h is not skew Hermitian of odd rank, discriminant

$$\mathrm{disc}\,\mathrm{Tr}_{L/K}h = (\mathrm{disc}\, L/K)^n \mathrm{N}_{L/K}(\mathrm{disc}\, h).$$

If h is Hermitian, we also have

$$\det \mathrm{Tr}_{L/K}h = (\det L_0/K_0)^n \mathrm{N}_{L_0/K_0}(\det h).$$

[9] That is to say, if the involution on L is $\neq$ the identity, then it is also $\neq$ the identity on K.

Assume first that $\dim_L V = 1$, say with basis vector v. Let $\lambda_1, \ldots, \lambda_l$ be a basis of L_0/K_0; it is also a basis of L/K and $\lambda_1 v, \ldots, \lambda_l v$ is a basis of V over K. (Note that if $K \neq K_0$, say $K = K_0(\sqrt{\delta})$, then $L \neq L_0$ and $L = L_0(\sqrt{\delta})$.) If $h(v,v)\lambda_i = \sum_k \alpha_{ik}\lambda_k$ where $\alpha_{ik} \in K_0$ for all i and k, then the matrix of the transfer $\mathrm{Tr}_{L/K} h$ is

$$\begin{aligned}\Big(\mathrm{Tr}_{L/K} h(\lambda_i v, \lambda_j v)\Big) &= \Big(\mathrm{Tr}_{L/K}(h(v,v)\lambda_i\lambda_j)\Big) = \Big(\mathrm{Tr}_{L/K} \sum_k \alpha_{ik}\lambda_k\lambda_j\Big) \\ &= \Big(\sum_k \alpha_{ik} \mathrm{Tr}_{L/K} \lambda_k\lambda_j\Big) = (\alpha_{ik})\big(\mathrm{Tr}_{L/K}\lambda_k\lambda_j\big).\end{aligned}$$

Now $\det(\alpha_{ik}) = \mathrm{N}_{L/K} h(v,v)$ and $\det\big(\mathrm{Tr}_{L/K}\lambda_k\lambda_j\big) = \det L/K$ – these are standard facts of the theory of fields – and so the proof of the determinant formula in this case is complete, and the proof for general n follows easily by choosing an orthogonal basis $v_1, \ldots, v_n$ of V. (We note as well that $\det L/K = \det L_0/K_0$, $\operatorname{disc} L/K = \operatorname{disc} L_0/K_0$, and, if h is Hermitian, $\mathrm{N}_{L/K} h(v,v) = \mathrm{N}_{L_0/K_0} h(v,v)$ since $\lambda_1, \ldots, \lambda_l$ is a basis of L_0/K_0).

The formula for discriminants follows easily from that for determinants. □

This lemma and its proof are adaptations of those for the bilinear case in Lemma 2.2, [50].

Corollary 1.5.1 (Dedekind's discriminant formula) *Let M be a midfield of the finite separable extension L/K. Then*

$$\operatorname{disc} L/K = (\operatorname{disc} M/K)^{(L:M)} \mathrm{N}_{M/K} \operatorname{disc} L/M.$$

This is proved by applying the lemma to the formula

$$\mathrm{Tr}_{L/K}\langle 1\rangle = \mathrm{Tr}_{M/K}(\mathrm{Tr}_{L/M}\langle 1\rangle). \qquad \square$$

Let $\mathrm{t} : (L, {}^-) \to (K, {}^-)$ be an involution trace (p. 35).

Theorem 1.5.10 *Suppose that L/K is an Abelian extension of local fields and that the involution ${}^-$ on L is $\neq \mathrm{id}$. If h_1 and h_2 are inequivalent nonsingular Hermitian forms over $(L, {}^-)$, then their traces $\mathrm{t}h_1$ and $\mathrm{t}h_2$ are also inequivalent.*

We first prove the following special case.

Lemma 1.5.7 *Suppose that the fixed field L_0 of the involution on L is $= K$. If h_1 and h_2 have the same rank but different determinants, then the symmetric bilinear forms $\mathrm{t}h_1$ and $\mathrm{t}h_2$ have the same rank and determinant but different Hasse invariants.*

Note that $\mathrm{t}(h_1 \perp h_2) = \mathrm{t}h_1 \perp \mathrm{t}h_2$. Because Hermitian forms over L are classified by rank and discriminant (cf. Table 1, p. 61), $h_i \cong \langle 1, \ldots, 1, \det h_i\rangle$ and so by Lemma 1.5.1(b),

$$\mathrm{s}(\mathrm{t}h_i) = \mathrm{s}(\mathrm{t}\langle 1, \ldots, 1\rangle) \cdot \mathrm{s}(\mathrm{t}\langle \det h_i\rangle) \cdot (\det \mathrm{t}\langle 1, \ldots, 1\rangle,\ \det \mathrm{t}\langle \det h_i\rangle)_K.$$

It follows that it suffices to prove the lemma in the case that h_1 has rank 1.

So suppose $h_1 = \langle\alpha\rangle$, say $h_1(v,v) = \alpha \in K$. Write $L = K(\sqrt{\delta})$. By (1.44), $\mathrm{t}(\sqrt{\delta}) = 0$ and so $\mathrm{t}(1) \neq 0$. Then $\mathrm{t}h_1 = \langle \alpha\mathrm{t}(1), -\alpha\delta\mathrm{t}(1)\rangle$ in the K-basis $v, \sqrt{\delta}v$ of

V. Thus $\det \mathrm{t}h_1 = -\delta$ which is independent of α. So $\mathrm{t}h_1$ and $\mathrm{t}h_2$ have the same determinant. Furthermore the Hasse invariant of $\mathrm{t}h_1$ is

$$\mathrm{s}(\mathrm{t}h_1) = (\alpha\mathrm{t}(1), -\alpha\delta\mathrm{t}(1))_K = (\alpha\mathrm{t}(1), \delta)_K$$

by identity (c) on p. 16. This *does* depend on the choice of α since δ is a nonsquare in K (cf. Ex. 4, p. 17). It follows that $\mathrm{t}h_1$ and $\mathrm{t}h_2$ have different Hasse invariants since there are only two possible determinants because $[\dot{K} : \mathrm{N}_{L/K}\dot{L}] = 2$ (cf. (1.23)). □

For the moment we assume the following theorem.

Theorem 1.5.11 *Suppose that L/K is a finite Abelian extension of local fields and $\mathrm{t} : L \to K$ is a nonzero K-linear map. If $b, b' : V \times V \to L$ are nonsingular symmetric bilinear forms with the same discriminant but different Hasse invariants, then their traces $\mathrm{t}b$ and $\mathrm{t}b'$ are not equivalent.*

This theorem is due to J. Milnor [50] in the more general case when L/K is finite and separable.

We now show that Theorem 1.5.10 follows from this theorem and Lemma 1.5.7.

Suppose first that the (nonidentity) involution $^-$ on L is the identity on K, and that L_0 is the subfield of L of elements fixed by it. We have $L = L_0 \oplus L_0\sqrt{\delta}$ for some $\delta \in \dot{L}_0$. Thus if $\alpha_0 \in L_0$, $\mathrm{t}\left(\overline{\alpha_0\sqrt{\delta}}\right) = -\mathrm{t}(\alpha_0\sqrt{\delta}) = \overline{\mathrm{t}(\alpha_0\sqrt{\delta})} = \mathrm{t}(\alpha_0\sqrt{\delta})$. Therefore $\mathrm{t}(L_0\sqrt{\delta}) = 0$ and we can factor t through the projection $\pi : L = L_0 \oplus L_0\sqrt{\delta} \to L_0$: $\mathrm{t} = \mathrm{s}\pi$ where $\mathrm{s} = \mathrm{t}|_{L_0}$. Note that $\pi(\bar{\alpha}) = \pi(\alpha)$ for all $\alpha \in L$, so π is an involution trace.

By the lemma, the symmetric bilinear forms πh_1 and πh_2 over L_0 have the same rank and discriminant but different Hasse invariants. Therefore by Theorem 1.5.11 the symmetric forms $\mathrm{s}\pi h_1 = \mathrm{t}h_1$ and $\mathrm{s}\pi h_2 = \mathrm{t}h_2$ are not equivalent.

Suppose now that the involution is *not* the identity on K. In this case we may assume that $\delta \in K_0$, and that $K = K_0(\sqrt{\delta})$. Let b_i be the nonsingular symmetric bilinear form $b_i(u, v) = h_i(u, v) + \overline{h_i(u, v)} = \mathrm{Tr}_{L/L_0}(h_i(u, v))$ over L_0. By Lem. 1.5.7, b_1 and b_2 have the same rank and determinant but different Hasse invariants. Let $\mathrm{t}_0 : L_0 \to K_0$ denote the restriction of t to L_0. By Theorem 1.5.11 t_0b_1 and t_0b_2 are not equivalent as symmetric forms over K_0. But

$$\mathrm{t}h_i(u, v) + \overline{\mathrm{t}h_i(u, v)} = \mathrm{t}b_i(u, v) = \mathrm{t}_0b_i(u, v),$$

and so $\mathrm{t}h_1$ and $\mathrm{t}h_2$ are not equivalent. This proves Theorem 1.5.10. □

We now proceed to the proof of Theorem 1.5.11.

The determinant of L/K is the determinant of the symmetric bilinear form $\mathrm{Tr}_{L/K}(\alpha\beta) : L \times L \to K$. For our purposes we need to consider the "t-determinant" of L/K, replacing $\mathrm{Tr}_{L/K}(\alpha\beta)$ by $\mathrm{t}(\alpha\beta)$:

$$\det{}_{\mathrm{t}} L/K = \det(\mathrm{t}(\alpha\beta)) = \det(\mathrm{t}(\lambda_i\lambda_j))$$

where $\lambda_1, \ldots, \lambda_l$ is a basis of L/K. It is well-defined $\bmod\, \dot{K}^2$. The proof of the following lemma is identical to that of Lem. 1.5.6 when the trace $\mathrm{Tr}_{L/K}$ is replaced by t.

Lemma 1.5.8 *If b is a symmetric form over L of dimension n, the determinant of the transfer $\mathrm{t}b$ over K is $(\det_{\mathrm{t}} L/K)^n \mathrm{N}_{L/K}(\det b)$.* □

Lemma 1.5.9 *In order to prove Theorem 1.5.11 it suffices to find two nonsingular symmetric forms b_1 and b_2 over L with the same rank and discriminant but with* $\mathrm{s}(\mathrm{t}b_1) \neq \mathrm{s}(\mathrm{t}b_2)$ ($\mathrm{s} =$ *the Hasse invariant*).

Since $\mathrm{t}b_1$ is not equivalent with $\mathrm{t}b_2$, b_1 and b_2 are also nonequivalent, and so their Hasse invariants are different (cf. Table 1, p. 61). Now we claim that $b \perp b_1$ and $b' \perp b_2$ are equivalent. They certainly have the same rank and discriminant. As for their Hasse invariants, by Lemma 1.5.1(b),

$$\begin{aligned}\mathrm{s}(b \perp b_1) &= \mathrm{s}(b)\mathrm{s}(b_1)(\det b, \det b_1)_L \\ &= (-\mathrm{s}(b'))(-\mathrm{s}(b_1))(\det b', \det b_2)_L = \mathrm{s}(b' \perp b_2).\end{aligned}$$

Thus we also have $\mathrm{t}b \perp \mathrm{t}b_1 \cong \mathrm{t}b' \perp \mathrm{t}b_2$, so

$$\mathrm{s}(\mathrm{t}b)\mathrm{s}(\mathrm{t}b_1)(\det \mathrm{t}b, \det \mathrm{t}b_1)_K = \mathrm{s}(\mathrm{t}b')\mathrm{s}(\mathrm{t}b_2)(\det \mathrm{t}b', \det \mathrm{t}b_2)_K.$$

Since $(\det \mathrm{t}b, \det \mathrm{t}b_1)_K = (\det \mathrm{t}b', \det \mathrm{t}b_2)_K$ by Lem. 1.5.6, and $\mathrm{s}(\mathrm{t}(b_1) = -\mathrm{s}(\mathrm{t}(b_1)$, $\mathrm{s}(\mathrm{t}b) = -\mathrm{s}(\mathrm{t}b')$. □

We now proceed with the proof of Theorem 1.5.11. The proof is divided into 4 cases.

Case 1. L contains an element α_0 whose norm in K is nonsquare. By §1.2.5 there is $\beta \in K$ such that $(\beta, N_{L/K}\alpha_0)_K = -1$. Consider the binary space V_0 over L with symmetric form $b_0 = \langle \alpha, -\alpha\beta \rangle$ with respect to the orthogonal basis u_0, v_0, where $\alpha \in \dot{L}$ is to be determined. For any choice of α its determinant is $-\beta$. We now calculate the Hasse invariant of $\mathrm{t}b_0$, freely using Lem. 1.5.1 and the properties of $(\cdot,\cdot)_K$ on p. 53. Let b_0' respectively b_0'' be the restriction of b_0 to the subspace Lu_0 respectively Lv_0.

Choose an orthogonal basis for the space $(Lu_0, \mathrm{t}b_0')$ over K. Then $\mathrm{t}b_0' = \langle \alpha_1, \ldots, \alpha_d \rangle$ (where $d = (L : K)$) for certain $\alpha_i \in \dot{K}$. And there is an orthogonal basis for $(Lv_0, \mathrm{t}b_0'')$ in which $\mathrm{t}b_0'' = \langle -\alpha_1\beta, \ldots, -\alpha_d\beta \rangle$. If s' is the Hasse invariant of $\mathrm{t}b_0'$, that of $\mathrm{t}b_0''$ is

$$\begin{aligned}\mathrm{s}'' &= \prod_{i<j}(-\alpha_i\beta, -\alpha_j\beta)_K \\ &= \mathrm{s}'(-\beta, \alpha_1 \ldots \alpha_d)_K^{d-1}(-\beta, -\beta)_K^{d(d-1)/2}.\end{aligned}$$

Thus the Hasse invariant of $\mathrm{t}b_0$ is

$$\begin{aligned}\mathrm{s} &= \mathrm{s}'\mathrm{s}''(\alpha_1 \ldots \alpha_d, \alpha_1 \ldots \alpha_d(-\beta)^d)_K \\ &= (-\beta, \alpha_1 \ldots \alpha_d)_K^{2d-1}(-1, \alpha_1 \ldots \alpha_d)_K(-\beta, -\beta)_K^{d(d-1)/2} \\ &= (\beta, \alpha_1 \ldots \alpha_d)_K(-\beta, -\beta)_K^{d(d-1)/2}.\end{aligned}$$

By Lemma 1.5.8, $\alpha_1 \ldots \alpha_d = (\det_{\mathrm{t}} L/K)\mathrm{N}_{L/K}\alpha$. It follows that s is the product of $(\beta, \mathrm{N}_{L/K}\alpha)_K$ and a factor which is independent of α, so we get different values for s if we choose $\alpha = \alpha_0$ and $\alpha = 1$. By the foregoing lemma, this proves Theorem 1.5.11 in this case.

Case 2. L has degree 2 over K. Then $\mathrm{N}_{L/K}\dot{L}$ has index 2 in $\dot{K}$, while $\dot{K}^2$ has index ≥ 4. (cf. pp. 163, 167, [54]). Thus we can apply Case 1.

Case 3. L has odd degree over K. The norm of any nonsquare α_0 in K is an odd power of α_0 and so is not a square. Apply Case 1 again.

Case 4. L/K Abelian. There is a tower of fields

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_r = L$$

in which each successive extension K_{i+1}/K_i has prime degree.

Since $\mathrm{Hom}_K(L, K)$ is a one dimensional vector space over L (with the action $\lambda_1\psi(\lambda_2) = \psi(\lambda_1\lambda_2)$), there is a $\lambda_1 \in L$ such that $\mathrm{t}(\lambda) = \mathrm{Tr}_{L/K}(\lambda_1\lambda)$ for all $\lambda \in L$. Now if $b \ncong b'$, then certainly $\lambda_1 b \ncong \lambda_1 b'$. Apply Case 2 or 3 to get $\mathrm{Tr}_{L/K_{r-1}}(\lambda_1 b) \ncong \mathrm{Tr}_{L/K_{r-1}}(\lambda_1 b')$. Again apply Case 2 or 3 to get $\mathrm{Tr}_{L/K_{r-2}}(\lambda_1 b) \ncong \mathrm{Tr}_{L/K_{r-2}}(\lambda_1 b')$, and so on. Eventually we get $\mathrm{Tr}_{L/K}(\lambda_1 b) \ncong \mathrm{Tr}_{L/K}(\lambda_1 b')$, i.e. $\mathrm{t}b \ncong \mathrm{t}b'$. □

There are some sharper results for trace forms of local fields, due mainly to V.P. Gallagher [29] and M. Epkenhans [22].

1.5.7 Equivalence of reflexive forms over division algebras. Although forms over division algebras are not of direct interest to us as far as representations are concerned, they do nevertheless arise in the consideration of representations over fields. In particular it is important to determine the equivalence classes of Hermitian and skew Hermitian forms over a central division K-algebra with involution, when K is real closed, local or global. The following table gives invariants in all the "classical" cases, and is derived mainly from the table on p. 347, [65].

Table 1

Type	**finite**	**R**	**local**	**global**
symmetric	dim, det	dim, sgn	dim, det, s	Hasse Prin.
skew-symmetric	dim	dim	dim	dim
Herm/field	dim	dim, sgn	dim, det	dim, det, $\mathrm{sgn}_{\mathfrak{p}}$
Herm/quat	∄	dim, sgn	dim	dim, $\mathrm{sgn}_{\mathfrak{p}}$
skew-Herm/quat	∄	dim	dim, det	dim, det, b
Herm/skew(2nd kd)	∄	∄	∄	dim, det, $\mathrm{sgn}_{\mathfrak{p}}$

Explanations. 1. R stands for "real closed", s for the Hasse invariant, skew(2nd kd) for a division algebra with an involution of the second kind, b for the Bartels invariant (discussed below), and Hasse Prin. for the Hasse Principle (p. 55).

2. It is understood that in the case of forms over the quaternions, an involution of the 1st kind is conjugation *.

3. $\mathrm{sgn}_{\mathfrak{p}}$ (K global). The signature is only defined when $\mathrm{char}\, K = 0$, i.e. when K is a number field. In the above table it can be ignored when the characteristic is $\neq 0$. Assume that $\mathrm{char}\, K = 0$. There are three cases:

(i) *Quadratic extension K/K_0.* In this case the signature $\mathrm{sgn}_{\mathfrak{p}} h$ of an Hermitian form $h : V \times V \to (K, {}^-)$ is defined for real primes $\mathfrak{p}$ of K_0 (or the corresponding orders P of K_0 – cf. Prop. 1.4.1, p. 42) for which K/K_0 is definite, i.e. $K = K_0(\sqrt{\delta})$ with $\delta < 0$ at P. For such $\mathfrak{p}$, $K_{0\mathfrak{p}} \cong \mathbb{R}$, $K_{0\mathfrak{p}} \otimes_{K_0} K \cong \mathbb{C}$, and $\mathrm{sgn}_{\mathfrak{p}} h$ is the signature of the "classical" Hermitian form

$$h_{\mathfrak{p}} = h^{\mathbb{C}} : V^{\mathbb{C}} \times V^{\mathbb{C}} \to (\mathbb{C},\ ^*\ ).$$

(ii) *Quaternion division algebra $(D,\ ^*\ )$.* Here the signature $\mathrm{sgn}_{\mathfrak{p}} h$ of an Hermitian form $h : V \times V \to (D,\ ^*\ )$ is defined for the real primes $\mathfrak{p}$ of the center K (or the corresponding orderings of K) for which the quaternion algebra $K_\mathfrak{p} \otimes_K D$ is not split (and so is $\cong \mathbb{H}$). It is the signature of the Hermitian form

$$h_\mathfrak{p} = h^\mathbb{R} : V^\mathbb{R} \times V^\mathbb{R} \to (\mathbb{H},\ ^*\ ).$$

See p. 41.

(iii) *Noncommutative division algebra* $(D, ^-)$ *with an involution of the second kind.* The signature $\mathrm{sgn}_\mathfrak{p} h$ of an Hermitian form $h : V \times V \to (D, ^-)$ is defined for the real primes $\mathfrak{p}$ of K_0 for which $(K, ^-)$ is definite. If $\mathfrak{p}$ is such a prime,

$$K_{0\mathfrak{p}} \otimes_{K_0} D \cong (K_{0\mathfrak{p}} \otimes_{K_0} K) \otimes_K D = K_\mathfrak{P} \otimes_K D = D_\mathfrak{P}$$

where $\mathfrak{P}$ is the unique (complex) prime of K lying above $\mathfrak{p}$. The involution $\mathrm{id} \otimes ^-$ on $K_{0\mathfrak{p}} \otimes_{K_0} K = K_\mathfrak{P} \cong \mathbb{C}$ is complex conjugation $\ ^*\ $ and it follows that the involution algebra $(D_\mathfrak{P},\ ^* \otimes ^-)$ is $\cong (\mathrm{M}(d, \mathbb{C}),\ ^\sim\ )$ where

$$\widetilde{a} = b^{-1} a^{t*} b, \quad \text{for some } b \text{ satisfying } b^{t*} = b$$

(Th. 1.3.6(a), p. 30). Suppose that $h : V \times V \to (D, ^-)$ is a nonsingular Hermitian form, and that

$$h_\mathfrak{P} : V_\mathfrak{P} \times V_\mathfrak{P} \to (D_\mathfrak{P},\ ^* \otimes ^-) \cong (\mathrm{M}(d, \mathbb{C}),\ ^\sim\ ) \tag{1.46}$$

is its "completion" (extension of scalars from K to $\mathbb{C}$). If $\dim_D V = m$, by Th. 3.2.9 (p. 120) there is a matrix $\underline{h} \in \mathbf{GL}(md, \mathbb{C})$ such that

$$h_\mathfrak{P}(u, v) = u\underline{h}v^{t*}b \quad \text{for all } u, v \in \mathbb{C}^{d \times md}, \qquad \underline{h}^{t*} = \underline{h},$$

where we have identified $V_\mathfrak{P} = \mathbb{C} \otimes_K V$ with $\mathbb{C}^{d \times md}$. (The reader is advised to take this on faith at this point and return to it later when it becomes necessary in subsequent developments). Thus $\underline{h}$ is a nonsingular Hermitian matrix over $\mathbb{C}$; the signature $\mathrm{sgn}_\mathfrak{p}\, h$ is defined to be the signature of the corresponding Hermitian form

$$\breve{h} : \mathbb{C}^{md} \times \mathbb{C}^{md} \to (\mathbb{C},\ ^*\ ), \qquad \breve{h}(u, v) = u\underline{h}v^{t*}.$$

This definition depends on the identification of $D_\mathfrak{P}$ with $\mathrm{M}(d, \mathbb{C})$ and the choice of b. As we have defined it, a different identification and choice of b would lead to the matrix $\alpha c_0 \underline{h} c_0^{t*}$ instead of $\underline{h}$, where $\alpha \in \dot{\mathbb{R}}$ and $c_0 \in \mathbf{GL}(md, \mathbb{C})$, by Th. 3.2.10 (p. 125). Thus with a change in the identification and the choice of b, $\mathrm{sgn}\, h_\mathfrak{p}$ will either be the same (if $\alpha > 0$) or will change sign. Therefore if h' is another Hermitian form of the same rank, $\mathrm{sgn}\, h_\mathfrak{p}$ and $\mathrm{sgn}\, h'_\mathfrak{p}$ will be equal with a particular choice of an identification and b if and only if they are equal with any other choice.

The definition of $\mathrm{sgn}_\mathfrak{p} h$ given by Scharlau on pp. 375-376 in [65] is the same as that given here. He defines the form $h_\mathfrak{P}$ as above, and then "scales" it by b^{-1} : $(h_\mathfrak{P} b^{-1})(u, v) = h_\mathfrak{P}(u, v)b^{-1}$. This scaled form is an Hermitian form over $(\mathrm{M}(d, \mathbb{C}),\ ^{t*}\ )$. It is then noted that it can be expressed by an Hermitian matrix in $\mathbb{C}^{md \times md}$, which in fact is the matrix $\underline{h}$ defined above.

4. The results on Hermitian forms over $(K, ^-)$ can be applied to the skew Hermitian case since if h is skew Hermitian over $(K, ^-)$, $\sqrt{\delta}h$ is Hermitian ($K = K_0(\sqrt{\delta})$). Similarly skew Hermitian forms over a central division algebra $(D, ^-)$ with an involution of the 2nd kind over a global field K, can be scaled by $\sqrt{\delta}$ to get Hermitian forms over $(D, ^-)$.

5. Suppose $(D, {}^-)$ is a quaternion division algebra with an orthogonal involution. The pure quaternions D_0 are stable under any involution since

$$\dot{D}_0 = \{d \in D : \ d \notin K,\ d^2 \in K\},$$

and so the 1-eigenspace $(D_0)_1$ of ${}^-$ has dimension 2 and $(D_0)_{-1}$ has dimension 1. This means that i, j and k can be chosen so that $\bar{i} = -i$, $\bar{j} = j$ and $\bar{k} = k$, and this in turn implies that $\bar{d} = i^{-1}d^*i$ for all $d \in D$.

Now suppose h is an Hermitian form over $(D, {}^-)$. Then hi (defined like hb^{-1} in 3.) is a skew Hermitian form over $(D, {}^*)$ and it is straightforward to check that the correspondence $h \leftrightarrow hi$ is bijective between Hermitian forms over $(D, {}^-)$ and skew Hermitian forms over $(D, {}^*)$, and also between skew Hermitian forms over $(D, {}^-)$ and Hermitian forms over $(D, {}^*)$. These are in fact category isomorphisms.

Thus statements concerning equivalence of ε-Hermitian forms over a quaternion algebra with conjugation as involution apply equally well to $-\varepsilon$-Hermitian forms over the same algebra with an orthogonal involution.

6. In the case of (nonsingular) skew Hermitian forms over quaternion algebras over local fields, we note that the determinant takes its values in $\dot{K}/\dot{K}^2$ and that furthermore it can take on *any* value if the dimension is > 1, while it misses the single value $(-1)\dot{K}^2$ when the dimension is 1. This, and the fact that dim and det characterize equivalence in this case, constitute “Tsukamoto’s Theorem” (p. 363, [65]).

7. The Hasse Principle and the Bartels Invariant. The Hasse Principle applies in all cases in the above table except skew Hermitian forms over a quaternion division algebra over a global field with involution = conjugation, that is to say, it is possible for forms in this case to be locally equivalent at all primes but not globally equivalent. In fact if D is the quaternion algebra in question and s is the number of primes $\mathfrak{p}$ of K at which $D_\mathfrak{p}$ is not split, then the number of global equivalence classes which correspond to a single local equivalence class is 2^{s-2} – thus the Hasse Principle holds if and only if $s = 2$ (the minimum number if D is not split). See [65], §§10.4.5 – 10.4.7, pp. 370-371. If h and g are skew Hermitian forms over $(D, {}^*)$, then (“Bartels theorem”) it can be shown that they are equivalent if and only if they have the same rank and determinant (or are locally equivalent at each prime $\mathfrak{p}$ of K) and have the same Bartels invariant $\mathrm{b}(h, g) \in \mathrm{Br}(K)/\langle[D]\rangle$. See [3] or [65] for its definition. We give its properties later on p. 203.

The remaining cases, in which the Hasse Principle *does* hold, require a little explanation. The symmetric case is of course the classical case, while the skew symmetric case is trivial since nonsingular forms of the same dimension over any field are equivalent. Hermitian forms over a division algebra with an involution of the second kind are covered in 10.6.1, [65].

Now consider the case of Hermitian forms over a nonsplit quaternion algebra $(D, {}^*)$ with conjugation as involution, say $D = (\alpha, \beta)_K$. Let h and g be nonsingular Hermitian forms over $(D, {}^*)$, and suppose that[10] $h_\mathfrak{p} \cong g_\mathfrak{p}$ for all primes $\mathfrak{p}$ of K.

[10] If $D_\mathfrak{p}$ is split, so $\cong \mathrm{M}(2, K_\mathfrak{p})$, then $h_\mathfrak{p}$ is an Hermitian form over a matrix algebra – such forms are dealt with in detail in Ch. 3.

Since the diagram

$$\begin{tikzcd} D \arrow[r] \arrow[d, "\mathrm{trd}"'] & D_{\mathfrak{p}} \arrow[d, "\mathrm{trd}"] \\ K \arrow[r] & K_{\mathfrak{p}} \end{tikzcd}$$

is commutative, the trace forms satisfy $(\operatorname{trd} h)_{\mathfrak{p}} \cong \operatorname{trd} h_{\mathfrak{p}}$ and so $(\operatorname{trd} h)_{\mathfrak{p}} \cong (\operatorname{trd} g)_{\mathfrak{p}}$ for all $\mathfrak{p}$ which, since these are symmetric bilinear forms, implies that $\operatorname{trd} h \cong \operatorname{trd} g$ and so $h \cong g$ by Jacobson's Theorem (p. 49).

An entirely similar proof works in the case of Hermitian forms over $(K, {}^{-})$. □

Existence theorems. We record here conditions for the existence of symmetric forms over local and global fields.

Theorem 1.5.12 *Let V be a vector space of dimension ≥ 2 over the local field K. Suppose that $(\alpha\dot{K}^2, \varepsilon) \in (\dot{K}/\dot{K}^2) \times \{\pm 1\}$ is given. Then there is a symmetric bilinear form $b : V \times V \to K$ with $\det b = \alpha$ and $\mathrm{s}(b) = \varepsilon$ if and only if $\varepsilon = 1$ when $\dim V = 2$ and $\alpha =_2 -1$.*

This is essentially 63:23, p. 171, [54]. (Of course b is unique up to equivalence by Table 1, p. 61). □

Theorem 1.5.13 *Suppose that for each prime $\mathfrak{p}$ of the global field K, $(U_{\mathfrak{p}}, f_{\mathfrak{p}})$ is a symmetric space over $K_{\mathfrak{p}}$ of the same dimension for each $\mathfrak{p}$. In order that there exist a symmetric space (V, b) over K such that $(V_{\mathfrak{p}}, b_{\mathfrak{p}}) \cong (U_{\mathfrak{p}}, f_{\mathfrak{p}})$ for each $\mathfrak{p}$, it is necessary and sufficient that there exists $d \in K$ such that $\det f_{\mathfrak{p}} \equiv d \bmod \dot{K}_{\mathfrak{p}}^2$ for each $\mathfrak{p}$, that $\mathrm{s}_{\mathfrak{p}} f_{\mathfrak{p}} = 1$ for all but finitely many $\mathfrak{p}$, and that $\prod_{\mathfrak{p}} \mathrm{s}_{\mathfrak{p}} f_{\mathfrak{p}} = 1$.*

This is proved for algebraic number fields (of finite degree over $\mathbb{Q}$) in 72:1, p. 203, [54], and the proof there can be easily seen to extend to global fields (of characteristic $\neq 2$, of course). We leave it as an exercise to show that the condition $\prod_{\mathfrak{p}} \mathrm{s}_{\mathfrak{p}} f_{\mathfrak{p}} = 1$, using the slightly different definition of the Hasse invariant there, is equivalent to the same relation using our definition. □

1.6 Grothendieck groups

Suppose that $(\mathbf{M}, +)$ is an Abelian monoid – that is to say $\mathbf{M}$ has a binary law of composition $x+y$ which is commutative and associative. Then we can construct a group $\mathrm{K}(\mathbf{M})$ called the *Grothendieck group of* $\mathbf{M}$ as follows (an alternative approach can be found in §7, Ch.1, [41]).

Take the set of ordered pairs $\mathbf{M} \times \mathbf{M}$ and say that two pairs (x_1, y_1) and (x_2, y_2) are related, $(x_1, y_1) \sim (x_2, y_2)$, if there is $z \in \mathbf{M}$ such that $x_1 + y_2 + z = x_2 + y_1 + z$. This is easily seen to be an equivalence relationship.

Denote the equivalence class of (x_1, y_1) by $[x_1, y_1]$, and let $\mathrm{K}(\mathbf{M})$ be the set of equivalence classes. It can be made into an Abelian group as follows. (One should intuitively think of $[x_1, y_1]$ as the difference $x_1 - y_1$). Addition in $\mathrm{K}(\mathbf{M})$ is defined by

$$[x_1, y_1] + [x_2, y_2] = [x_1 + x_2, y_1 + y_2],$$

and is easily seen to be well-defined, associative and commutative. The equivalence class $[x, x]$ for any $x \in \mathbf{M}$ is a 0 for addition – note that $[x, x] = [y, y]$ for all $x, y \in \mathbf{M}$. And $[y, x]$ is the negative of $[x, y]$ since $[x, y] + [y, x] = [x + y, x + y] = 0$. Thus $\mathrm{K}(\mathbf{M})$ *is* an Abelian group.

Since $[x+y,y]=[x+z,z]$ for all $x,y,z \in M$, the map $\iota : \mathbf{M} \to \mathrm{K}(\mathbf{M})$ given by $\iota(x)=[x+y,y]$ for any $y \in \mathbf{M}$ is well-defined. It is a homomorphism, and

$$[x_1,y_1]=[x_1+2z,y_1+2z]=[x_1+z,z]+[z,y_1+z]=\iota(x_1)-\iota(y_1).$$

Thus the image of $\mathbf{M}$ generates $\mathrm{K}(\mathbf{M})$ as an Abelian group.

We note that

$$\iota \text{ is injective if and only if } \mathbf{M} \text{ has cancellation.} \tag{1.47}$$

Indeed $\iota(x_1)=\iota(x_2)$ if and only if $x_1+2y+z=x_2+2y+z$ for some y and z, which implies that $x_1=x_2$ if $\mathbf{M}$ has cancellation. Conversely suppose $x_1+z=x_2+z$. Then $\iota(x_1)=[x_1+z,z]=[x_2+z,z]=\iota(x_2)$, so $x_1=x_2$ if ι is injective.

$\mathrm{K}(\mathbf{M})$ has a universal mapping property:

Proposition 1.6.1 *Let $\varphi : \mathbf{M} \to A$ be a homomorphism of $\mathbf{M}$ into an Abelian group A. Then there is a unique homomorphism $\widehat{\varphi} : \mathrm{K}(\mathbf{M}) \to A$ making*

$$\begin{tikzcd}
& \mathrm{K}(\mathbf{M}) \arrow[d, "\widehat{\varphi}"] \\
\mathbf{M} \arrow[ur, "\iota"] \arrow[r, "\varphi"] & A
\end{tikzcd} \tag{1.48}$$

commutative.

If $[x_1,y_1]=[x_2,y_2]$, say $x_1+y_2+z=x_2+y_1+z$, then applying φ to this equation and cancelling $\varphi(z)$ leads to $\varphi(x_1)-\varphi(y_1)=\varphi(x_2)-\varphi(y_2)$. Thus we may define

$$\hat{\varphi}[x_1,y_1]=\varphi(x_1)-\varphi(y_1).$$

It is straightforward to check that this *is* a homomorphism $\mathrm{K}(\mathbf{M}) \to A$ and that it makes (1.48) commutative. Furthermore if $\psi : \mathrm{K}(\mathbf{M}) \to A$ is another homomorphism such that $\psi\iota=\varphi$, then $\psi[x_1,y_1]=\psi(\iota(x_1))-\psi(\iota(y_1))=\hat{\varphi}[x_1,y_1]$, i.e. $\psi=\hat{\varphi}$. □

In the usual way, one gets:

Corollary 1.6.1 K *is a functor from the category of Abelian monoids to the category of Abelian groups.* □

A commutative monoid is a *commutative semiring* if it has, in addition to the sum $x+y$, a product xy which is associative, commutative and distributive over addition.

Proposition 1.6.2 *Let $\mathbf{S}$ be a commutative semiring.*

(a) The product

$$[x_1,y_1]\cdot[x_2,y_2]=[x_1x_2+y_1y_2,\ x_1y_2+y_1x_2] \tag{1.49}$$

makes $\mathrm{K}(\mathbf{S})$ into a commutative ring (without a multiplicative identity, in general), and $\iota : \mathbf{S} \to \mathrm{K}(\mathbf{S})$ is a semiring homomorphism. If $1_{\mathbf{S}}$ is a multiplicative identity of $\mathbf{S}$, then $\iota(1_{\mathbf{S}})$ is a multiplicative identity for $\mathrm{K}(\mathbf{S})$. If in addition $\mathbf{H}$ is a nonempty subset of $\mathbf{S}$ with the property $\mathbf{SH} \subset \mathbf{H}$, then the subgroup $\langle \iota\mathbf{H} \rangle$ of $\mathrm{K}(\mathbf{S})$ generated by $\iota\mathbf{H}$ is an ideal of $\mathrm{K}(\mathbf{S})$.

(b) Let $\mathbf{M}$ be an Abelian monoid, and $\mathbf{S} \times \mathbf{M} \to \mathbf{M}$, $(s,x) \to sx$, a map satisfying

$$s(x+y)=sx+sy, \quad (s+t)x=sx+tx, \quad s(tx)=(st)x$$

for all $x, y \in \mathbf{M}$ and all $s, t \in \mathbf{S}$. Then

$$[s,t][x,y] = [sx+ty, tx+sy] \tag{1.50}$$

makes $\mathrm{K}(\mathbf{M})$ *into a* $\mathrm{K}(\mathbf{S})$*-module. If $1_{\mathbf{S}}$ is a multiplicative identity of $\mathbf{S}$ satisfying $1_{\mathbf{S}}x = x$ for all $x \in \mathbf{M}$, then the multiplicative identity $\iota 1_{\mathbf{S}}$ of* $\mathrm{K}(\mathbf{S})$ *satisfies $\iota 1_{\mathbf{S}}[x,y] = [x,y]$ for all $[x,y] \in \mathrm{K}(\mathbf{M})$.*

The proof is long but straightforward. We simply sketch the proof of (b) and leave the details (and (a)) as an exercise.

One first shows that (1.50) is well-defined by showing that if $[x,y] = [x',y']$ respectively $[s,t] = [s',t']$, then $[sx'+ty', tx'+sy'] = [sx+ty, tx+sy]$ respectively $[s'x+t'y, t'x+s'y] = [sx+ty, tx+sy]$. One then easily verifies the module axioms

$$\begin{aligned}
[s,t]\left([x,y]+[x',y']\right) &= [s,t][x,y]+[s,t][x',y'],\\
\left([s,t]+[s',t']\right)[x,y] &= [s,t][x,y]+[s',t'][x,y],\\
[s,t]\left([s',t'][x,y]\right) &= \left([s,t][s',t']\right)[x,y]
\end{aligned}$$

and the fact that $\iota 1_{\mathbf{S}}$ has the stated property. □

We also need a "graded" version of the Grothendieck group. Suppose that $\mathbf{M}$ is a direct sum $\mathbf{M} = \bigoplus_\nu \mathbf{M}_\nu$ of submonoids, where ν runs over an indexing set N. The direct sum here means that every element of $\mathbf{M}$ is a sum of a finite number of elements, each from a different "homogeneous component" $\mathbf{M}_\nu$, in one and only one way. (If $\mathbf{M}$ contains a zero element, the requirement is that every *nonzero* element of $\mathbf{M}$ is a sum of a finite number of nonzero elements, each from a different homogeneous component, in one and only one way).

Proposition 1.6.3 *(a)* $\mathrm{K}(\mathbf{M})$ *is also graded by N,* $\mathrm{K}(\mathbf{M}) = \bigoplus \mathrm{K}(\mathbf{M})_\mu$*, in such a way that for all ν, $\mathrm{K}(\mathbf{M})_\nu$ is the Grothendieck group $\mathrm{K}(\mathbf{M}_\nu)$, and the canonical homomorphism $\iota : \mathbf{M} \to \mathrm{K}(\mathbf{M})$ is graded – i.e. $\iota(\mathbf{M}_\nu) \subset \mathrm{K}(\mathbf{M})_\nu$. In fact $\iota|_{\mathbf{M}_\nu}$ is the canonical map $\mathbf{M}_\nu \to \mathrm{K}(\mathbf{M}_\nu)$.*

(b) Suppose in addition that $\mathbf{H}$ is a graded subset of $\mathbf{M}$ in the sense that every element of $\mathbf{H}$ is a finite sum of elements, each from a different $\mathbf{H}_\nu := \mathbf{H} \cap \mathbf{M}_\nu$. The subgroups $\langle \iota\mathbf{H}\rangle$ of $\mathrm{K}(\mathbf{M})$ and $\langle \iota\mathbf{H}_\nu\rangle$ of $\mathrm{K}(\mathbf{M})_\nu$ satisfy

$$\langle \iota\mathbf{H}\rangle = \oplus_\nu \langle \iota\mathbf{H}_\nu\rangle$$

and so

$$\mathrm{K}(\mathbf{M})/\langle \iota\mathbf{H}\rangle \cong \oplus_\nu \left(\mathrm{K}(\mathbf{M}_\nu)/\langle \iota\mathbf{H}_\nu\rangle\right).$$

Define $\mathrm{K}'(\mathbf{M}) = \oplus_\nu \mathrm{K}(\mathbf{M}_\nu)$. Let $\varphi : \mathbf{M} \to A$ be a homomorphism into an Abelian group A, and put $\varphi_\nu = \varphi|_{\mathbf{M}_\nu}$. By the universal mapping property of $\mathrm{K}(\mathbf{M}_\nu)$, there is a unique homomorphism $\widehat{\varphi}_\nu : \mathrm{K}(\mathbf{M}_\nu) \to A$ making

$$\begin{tikzcd}
 & \mathrm{K}(\mathbf{M}_\nu) \arrow[d, "\widehat{\varphi}_\nu"] \\
\mathbf{M}_\nu \arrow[ur, "\iota_\nu"] \arrow[r, "\varphi_\nu"] & A
\end{tikzcd}$$

commutative, where ι_ν is the canonical map. Define $\widehat{\varphi} = \oplus_\nu \widehat{\varphi}_\nu : \mathrm{K}'(\mathbf{M}) \to A$ and $\iota' = \oplus_\nu \iota_\nu : \mathbf{M} \to \mathrm{K}'(\mathbf{M})$. Since $\iota'\mathbf{M}$ generates $\mathrm{K}'(\mathbf{M})$, it is clear that $\widehat{\varphi}$ is the unique map making

$$\begin{tikzcd}
 & \mathrm{K}'(\mathbf{M}) \arrow[d, "\widehat{\varphi}"] \\
\mathbf{M} \arrow[ur, "\iota'"] \arrow[r, "\varphi"] & A
\end{tikzcd}$$

commutative, so $\mathbf{M} \overset{\iota'}{\to} \mathrm{K}'(\mathbf{M})$ has the same universal mapping property as $\mathbf{M} \to \mathrm{K}(\mathbf{M})$. By the usual argument involving universal mapping properties in the diagrams

$$\begin{tikzcd}
 & \mathrm{K}'(\mathbf{M}) \arrow[dd, "\widehat{\iota}"] & & & \mathrm{K}'(\mathbf{M}) \\
\mathbf{M} \arrow[ur, "\iota'"] \arrow[dr, "\iota"] & & & \mathbf{M} \arrow[ur, "\widehat{\iota}'"] \arrow[dr, "\iota"] & \\
 & \mathrm{K}(\mathbf{M}), & & & \mathrm{K}(\mathbf{M}), \arrow[uu, "\widehat{\iota'}"]
\end{tikzcd}$$

$\widehat{\iota}$ and $\widehat{\iota'}$ are mutually inverse isomorphisms. It follows that

$$\mathrm{K}(\mathbf{M}) = \oplus_\nu \widehat{\iota}\mathrm{K}(\mathbf{M}_\nu) = \oplus_\nu \mathrm{K}(\mathbf{M}_\nu)$$

(after identification) and that $\iota|_{\mathbf{M}_\nu}$ is the canonical map $\mathbf{M}_\nu \to \mathrm{K}(\mathbf{M}_\nu)$.

Now (b). Since $\iota\mathbf{H} \subset \sum_\nu \iota\mathbf{H}_\nu$, $\langle\iota\mathbf{H}\rangle \subset \sum_\nu \langle\iota\mathbf{H}_\nu\rangle$, and therefore $\langle\iota\mathbf{H}\rangle = \sum_\nu \langle\iota\mathbf{H}_\nu\rangle$. Since $\langle\iota\mathbf{H}_\nu\rangle \subset \langle\iota\mathbf{M}_\nu\rangle = \mathrm{K}(\mathbf{M})_\nu$, we get $\sum_\nu \langle\iota\mathbf{H}_\nu\rangle = \oplus_\nu \langle\iota\mathbf{H}_\nu\rangle$. □

Now assume further that $\mathbf{S}$ is a commutative semiring with a multiplicative identity, and that $(\mathsf{N}, +)$ is an Abelian monoid such that $\mathbf{S} = \oplus_\nu \mathbf{S}_\nu$ and $\mathbf{S}_\nu \mathbf{S}_\mu \subset \mathbf{S}_{\nu+\mu}$ for all $\nu, \mu \in \mathsf{N}$. It is straightforward to check the following graded version of Prop. 1.6.2.

Proposition 1.6.4 *The graded Abelian group* $\mathrm{K}(\mathbf{S}) = \oplus_\nu \mathrm{K}(\mathbf{S}_\nu)$ *is a graded commutative ring, satisfying* $\mathrm{K}(\mathbf{S}_\nu)\mathrm{K}(\mathbf{S}_\mu) \subset \mathrm{K}(\mathbf{S}_{\nu+\mu})$ *for all* $\nu, \mu \in \mathsf{N}$. *Furthermore if the graded subset* $\mathbf{H}$ *satisfies* $\mathbf{SH} \subset \mathbf{H}$, *then* $\langle\iota\mathbf{H}\rangle$ *is a graded ideal* $\oplus_\nu \langle\iota\mathbf{H}_\nu\rangle$ *of* $\mathrm{K}(\mathbf{S})$, *and* $\mathrm{K}(\mathbf{S})/\langle\iota\mathbf{H}\rangle \cong \oplus_\nu \left(\mathrm{K}(\mathbf{S}_\nu)/\langle\iota\mathbf{H}_\nu\rangle\right)$ *is also a graded commutative ring.* □

Example. An important example of the Grothendieck group is $\mathrm{K}_0(R)$ where R is a ring. It is by definition the Grothendieck group $\mathrm{K}(\mathbf{P})$ where $\mathbf{P}$ is the Abelian monoid of isomorphism classes of finitely generated projective R-modules, with addition $[P_1] + [P_2] = [P_1 \oplus P_2]$.

Of special interest to us later is $\mathrm{K}_0(A)$ where A is a separable algebra over a field K. In this case every A-module is projective – see Th. 1.2.3, p. 6, and the definition of semisimple ring on the same page. By Th. 1.2.7, p. 8, $\mathbf{P}$ is graded by the set S of isomorphism classes of simple A-modules, and so $\mathrm{K}_0(A)$ is similarly graded by S. In fact by Th. 1.2.2(c) $\mathrm{K}_0(A)$ is the free Abelian group on these isomorphism classes, so is $\cong \mathbb{Z}^{|\mathsf{S}|}$. □

Exercises. 1. If R is the direct sum $R = R_1 \oplus R_2$ of two rings, show that there is a canonical isomorphism $K_0(R) \to K_0(R_1) \oplus K_0(R_2)$, taking $[P]$ to $([R_1P], [R_2P])$. (We identify $K_0(R)$ with $K_0(R_1) \oplus K_0(R_2)$ via this isomorphism).

2. Let $(R, ^{-})$ be a ring with involution. If $P \in \mathbf{P}$, then the map $[P] \to [\overline{P^*}]$ where $\overline{P^*}$ is the twisted dual, gives an involution, also denoted $^{-}$, of the Abelian group $\mathrm{K}_0(R)$.

3. Suppose $(A, ^{-})$ is a hyperbolic involution algebra, $A = A_1 \oplus A_2$ where $\overline{A_1} = A_2$. Show that
(i) $\overline{\mathrm{K}_0(A_1)} = K_0(A_2)$,
(ii) if A_1 is a simple algebra and V_1 and V_2 are A_1 respectively A_2-modules of the same length, $\overline{[V_1]} = [V_2]$.

4. Let $(A, ^{-})$ be a $(K, ^{-})$-involution algebra and $(L, ^{-})/(K, ^{-})$ an extension of fields with involution. Then there is a canonical map $\mathrm{K}_0(A) \to \mathrm{K}_0(L \otimes_K A)$ taking $[P] \to [L \otimes_K P]$ which commutes with the involutions.

5. (This exercise requires knowledge of §3.1.2). Assume A is a semisimple K-algebra with a $(K, ^{-})$-involution and $\varepsilon = \pm 1$. If $h : (V \oplus W) \times (V \oplus W) \to (A, ^{-})$ is an ε-hyperbolic form with V and W totally isotropic, then $\overline{[V]} = [W]$, and conversely, if $\overline{[V]} = [W]$, then there is an ε-hyperbolic form on $V \oplus W$ under which V and W are totally isotropic. □

Remark. The canonical map in 4. is injective if A is separable – cf. Exercise 6., p. 417, [19]. □

1.7 Linear representations of finite groups

References for this section are [68], [18], and [19]. The basic facts, with which we begin, can be found in §§1-3 of [68] and Chs. II and V of [18].

We assume throughout that G is a finite group of order $g = |G|$. All vector spaces over the field K are assumed to be finite dimensional.

1.7.1 Basic facts about linear representations. A *linear representation* – or simply *representation* – of G is a homomorphism

$$\rho : G \to \mathbf{GL}(V) \tag{1.51}$$

of G into the "general linear group" of the K-vector space V, the group of invertible K-linear transformations of V into itself. More precisely, ρ is a *K-linear representation of G*, or a *linear representation of G over K*. The dimension of V over K is called the *degree* of ρ.

Another linear representation $\rho' : G \to \mathbf{GL}(V')$ over K is *equivalent* to ρ if there is a K-linear isomorphism $\varphi : V \to V'$ making

$$\begin{tikzcd} V \arrow[r, "\varphi"] \arrow[d, "\rho(s)"'] & V' \arrow[d, "\rho'(s)"] \\ V \arrow[r, "\varphi"'] & V' \end{tikzcd} \tag{1.52}$$

commutative for all $s \in G$. Such an isomorphism is sometimes called an *equivariant* isomorphism, or more precisely a G-equivariant isomorphism, and we write $\rho \simeq \rho'$.

If a basis of V is chosen and P_s is the matrix of $\rho(s)$ with respect to the basis, the map $s \to \mathsf{P}_s$ is a *matrix representation* of G over K, $\mathsf{P} : G \to \mathbf{GL}(n, K)$.

The notion of representation of G can also be stated in terms of modules over the group algebra KG – V is a (finitely generated) KG-module via the action $sv = \rho(s)v$ of G on V, extended to KG by linearity:

$$(\sum_s \alpha_s s)v = \sum_s \alpha_s \rho(s)v.$$

We then refer to V as the KG-module *corresponding to* or *arising from* the representation ρ.

Conversely if V is a KG-module, of finite dimension over K (or equivalently, finitely generated over KG), we can define a map $\rho : G \to \mathrm{End}(V)$ by decreeing that $\rho(s)v = sv$. Then

$$\rho(s)(\rho(t)v) = s(tv) = (st)v = \rho(st)v$$

so $\rho(st) = \rho(s)\rho(t)$. Furthermore its image is in $\mathbf{GL}(V)$ since $\rho(s)\rho(s^{-1}) = \rho(1) = \mathrm{id}_V$, so ρ is a representation – we say that it is the representation *afforded* by the KG-module V.

The commutativity of the diagram (1.52) is equivalent to $s\varphi = \varphi s$. This means that φ is a KG-homomorphism, and so we see that *the representations ρ and ρ' are equivalent if and only if the KG-modules corresponding to them are isomorphic as KG-modules.*

Formally, there is an isomorphism between the category of K-representations of G of finite dimension and the category of finitely generated KG-modules.

In terms of the corresponding matrix representations, P and P' are equivalent if and only if there is an invertible matrix $\underline{\varphi}$ such that

$$\mathsf{P}'_s = \underline{\varphi}\mathsf{P}_\mathrm{s}\underline{\varphi}^{-1} \qquad \text{for all } s \in G.$$

Note that if $V = V'$, then $\varphi \in \mathbf{GL}(V)$ and (1.52) is equivalent to $\rho'(s) = \varphi\rho(s)\varphi^{-1}$, which is expressed as "ρ and ρ' are conjugate representations".

The connection between representations and modules allows us to introduce the notions and theory of modules into representation theory. Thus for example we get the notion of *subrepresentation* of ρ as the representation afforded by a KG-submodule of V, and the notion of the *direct sum* $\rho_1 \oplus \rho_2$ of two representations as the representation afforded by the direct sum $V_1 \oplus V_2$ of their modules. When V is simple as a KG-module, ρ is called *irreducible* (over K). If ρ is reducible over K, it means that there is a basis of V such that

$$\mathsf{P}_s = \begin{pmatrix} \mathsf{P}_{1,s} & * \\ 0 & \mathsf{P}_{2,s} \end{pmatrix},$$

where $\mathsf{P}_{1,s}$ and $\mathsf{P}_{2,s}$ are matrix representations of G afforded by a KG-submodule U of V and the factor module V/U respectively, 0 is a zero matrix of the appropriate size and $*$ is also a matrix of the appropriate size. Such a basis of V is obtained by taking a basis of the KG-submodule U and augmenting it to a basis of V.

If $V = V_1 \oplus V_2$ is the space of the direct sum $\rho_1 \oplus \rho_2$, then in a basis of V which is the union of bases of V_1 and V_2, the matrix P_s is the "direct sum" $\mathsf{P}_{1,s} \oplus \mathsf{P}_{2,s}$ of the matrices of $\rho_1(s)$ and $\rho_2(s)$:

$$\mathsf{P}_s = \begin{pmatrix} \mathsf{P}_{1,s} & 0 \\ 0 & \mathsf{P}_{2,s} \end{pmatrix}.$$

In this case one says that ρ or P is *decomposable* (assuming, of course, that V_1 and V_2 are $\neq 0$).

And when V is a semisimple KG-module, ρ is referred to as *completely reducible*, and there is a basis of V such that

$$\mathsf{P}_s = \begin{pmatrix} \mathsf{P}_{1,s} & 0 & \cdots & 0 \\ 0 & \mathsf{P}_{2,s} & \cdots & 0 \\ & & & \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & \mathsf{P}_{k,s} \end{pmatrix},$$

where the P_i are irreducible matrix representations.

Of particular importance is *Maschke's Theorem*:

Theorem 1.7.1 *The algebra KG is separable if and only if the order g of G is not divisible by the characteristic of the field K.*

The sufficiency (the most important part of the theorem and the only part we will use) is proved as follows. It is enough to prove that KG is semisimple, since then every scalar extension $L \otimes_K KG \cong LG$ (given by $\sum_s \alpha_s \otimes s \to \sum_s \alpha_s s$) would also be semisimple. By Th. 1.2.3 it is enough to show that any KG-submodule U of V splits V as a KG-module. It certainly splits V as a vector space; let $\pi : V \to U$ be the corresponding projection of such a splitting. Then one can check that the map

$$\widetilde{\pi} : V \to U, \quad \widetilde{\pi}(v) = \tfrac{1}{g} \sum_s s\pi(s^{-1}v)$$

is a KG-linear projection of V onto U, and so $V = U \oplus \ker \widetilde{\pi}$ is a splitting of V into KG-submodules. □

Thus when the characteristic does not divide g, or more generally when the representation ρ is completely reducible, the KG-module V is semisimple and so (Th. 1.2.2, p. 6) is the direct sum of its homogeneous components V_S and each of these homogeneous components is a direct sum of a uniquely determined (finite) number of simple submodules isomorphic to S. In representation-theoretic terms, this means that ρ is the direct sum of irreducible representations, and that the multiplicity of any particular equivalence class of irreducible representations in this direct sum is invariant.

The *tensor product* $\rho_1 \otimes \rho_2$ of two representations of G is defined as the representation afforded by the tensor product of their spaces $V_1 \otimes_K V_2$, with the action $s(v_1 \otimes v_2) = sv_1 \otimes sv_2$.

To put it another way, the tensor product $V_1 \otimes_K V_2$ of two KG-modules is, in a natural way, also a KG-module. It is easy to see that this implies a commutative semiring structure on the monoid $\mathbf{P}$ of isomorphism classes of KG-modules, and so by Prop. 1.6.2, p. 65, $\mathrm{K}_0(KG)$ is a ring – in fact with a 1 equal to the equivalence class $[K]$ of the trivial representation.

If L/K is any field extension, the inclusion $\mathbf{GL}(V) \overset{\iota}{\hookrightarrow} \mathbf{GL}(L \otimes_K V)$ leads to an L-representation

$$\rho^L = \iota \circ \rho : G \to \mathbf{GL}(L \otimes_K V) \tag{1.53}$$

– the representation obtained from ρ by *extending the scalars to L*. The LG-module corresponding to ρ^L is simply the module $L \otimes_K V = V^L$ on which LG operates naturally via the canonical isomorphism $LG \cong L \otimes_K KG$. (We usually identify LG and $L \otimes_K KG$ via this isomorphism.) Slightly more generally, using a homomorphism $\varphi : K \to L$ of fields, one obtains an L representation (1.53) by making L into a K-space via $\alpha.\lambda = \varphi(\alpha)\lambda,\ \alpha \in K, \lambda \in L$. This is also referred to as extending the scalars.

On the other hand if V is a finite dimensional vector space over L, a representation $\rho : G \to \mathbf{GL}(V)$ over L is said to be *defined over* the subfield K if an L-basis for V can be chosen so that the corresponding matrix representation $\mathsf{P} : G \to \mathbf{GL}(n, L)$ is over K, that is to say the entries of the matrix $\mathsf{P}(s)$ are in K for all $s \in G$, or equivalently that $\mathsf{P} : G \to \mathbf{GL}(n, K)$. This is also equivalent to the existence of a vector space V_0 over K and a representation $\rho_0 : G \to \mathbf{GL}(V_0)$ over K such that $\rho_0^L \simeq \rho$.

1.7.2 Characters. The *character* of a representation ρ over K is the map $\chi = \chi_\rho : G \to K$ which assigns to each $s \in G$ the trace of the K-linear transformation $\rho(s)$:

$$\chi_\rho(s) = \mathrm{tr}(\rho(s)).$$

χ is in the K-algebra of K-valued functions on G – in fact it is in the K-algebra of K-valued "class functions" of G – the functions constant on the conjugacy classes of G – since

$$\chi(tst^{-1}) = \chi(s)$$

for all $s, t \in G$. It is occasionally convenient to write $\chi_V = \chi_\rho$.

Characters satisfy

$$\chi_{\rho_1 \oplus \rho_2} = \chi_{\rho_1} + \chi_{\rho_2}, \quad \chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1}\chi_{\rho_2}, \quad \chi_V = \chi_U + \chi_W$$

if

$$0 \to U \to V \to W \to 0$$

is an exact sequence of KG-modules. Also

$$\chi(1) = (\dim V)1_K, \quad \chi(s^{-1}) = \chi(s)^*,$$

where $\chi(s)^*$ is the "complex conjugate" of $\chi(s)$. By this we mean the following: over an algebraically closed extension field, the linear transformation $\rho(s)$ has $n = \dim V$ eigenvalues (including multiplicities) all of which are g^{th} roots of unity, and $\mathrm{tr}(\rho(s))$ is their sum. Further, $\mathrm{tr}(\rho(s^{-1}))$ is the sum of the inverses of these eigenvalues and we refer to the process of taking the sum of their inverses as "complex conjugation".

Remark. If the field K has characteristic 0 and we identify, in any way, the maximal cyclotomic subextension of the prime field ("$\mathbb{Q}$") of K with the corresponding subfield of $\mathbb{C}$, this process *is* complex conjugation in the ordinary sense. But if K has characteristic $p \neq 0$, this process is not always induced by an element of the Galois group of some extension of K which contains the eigenvalues, and in fact even depends on the actual eigenvalues of $\rho(s)$ rather than just their sum. For example if K has characteristic 5, the elements $1, 2, 3, 4$ of the prime field are all 4^{th} roots of 1, and $2+4 = 3+3$ but $2^{-1}+4^{-1} = 3+4 \neq 3^{-1}+3^{-1} = 2+2$. However since the roots of unity which appear in the trace of $\rho(s)$ are uniquely determined as the eigenvalues of $\rho(s)$, the sum of their inverses is also uniquely determined by $\rho(s)$. □

It is clear also that if L/K is an extension field, then

$$\chi_{\rho^L} = \chi_\rho.$$

The central theorem of character theory is

Theorem 1.7.2 *If* char $K = 0$*, two representations of* G *over* K *are equivalent if and only if their characters are equal.* □

This is a very powerful theorem, and especially so since the character of a representation is often easily calculated.

The subring $\mathsf{X}_K(G)$ of the ring of K-valued functions on G, generated by the characters of representations over K, is called the *ring of virtual characters*, and it is clear that each virtual character is the difference $\chi_1 - \chi_2$ of two characters. When the characteristic is 0, the ring of virtual characters is canonically isomorphic to the Grothendieck group of K-representations of G, which is by definition the Grothendieck group of the monoid of equivalence classes $[\rho]$ of representations, with addition defined in the obvious way, $[\rho_1] + [\rho_2] = [\rho_1 \oplus \rho_2]$. The isomorphism is of course $[\rho] \to \chi_\rho$, and it respects the multiplication defined in both groups – namely $\chi_1\chi_2$ and $[\rho_1 \otimes \rho_2]$ – and so is an isomorphism of rings as well.

These rings are isomorphic to a third ring, namely $\mathrm{K}_0(KG)$, via the categorical isomorphism between representations of G over K and finitely generated KG-modules. The ring structure on $\mathrm{K}_0(KG)$ arises from the KG-action $s.(v_1 \otimes_K v_2) = sv_1 \otimes_K sv_2$ on the tensor product $V_1 \otimes_K V_2$ of two KG-modules. Of course it is essentially the same as the Grothendieck group of K-representations of G.

Many of these same properties are enjoyed by *Brauer characters*, which are defined in the case that K is a field of prime characteristic p, as follows. An element s of G is called *p-regular* if p does *not* divide the order of s, otherwise s is called *p-singular*. Assume that there is a field $\widetilde{K}$ of characteristic 0 with a discrete valuation whose ring of integers $\mathfrak{o}$ and prime ideal $\mathfrak{p}$ satisfy $\mathfrak{o}/\mathfrak{p} \cong K$ – there *is* always such a field if K is perfect – cf. p. 45, [66]. The triple $(\widetilde{K}, \mathfrak{o}, K)$ is called a *p-modular system* (cf. p. 419*ff*, [19]). We shall also assume that $\widetilde{K}$ is "sufficiently large" relative to G, meaning that it contains the group of all g^{th} roots of unity. Then K also is sufficiently large relative to G. Let $g = p^r m$ where $p \nmid m$. The residue class map $\mathfrak{o} \to K$ induces an isomorphism between the groups of m^{th} roots of unity in $\widetilde{K}$ and K; if $\zeta \in K$ is one of them, we denote by $\widetilde{\zeta}$ the corresponding root of unity in $\mathfrak{o}$.

Suppose now that ρ is a K-representation (1.51) of degree n and let $s \in G$ be a p-regular element. Since $\rho(s)^m = 1$, the eigenvalues $\zeta_1, \ldots, \zeta_n$ (with multiplicities) of $\rho(s)$ are m^{th} roots of unity and $\rho(s)$ is diagonalizable. The *Brauer character*[11] is defined for each p-regular element s of G by

$$\chi_\rho(s) = \widetilde{\zeta}_1 + \cdots + \widetilde{\zeta}_n \in \mathfrak{o}.$$

The *complex conjugate* $\chi_\rho(s)^*$ can be defined for a Brauer character as it was for an ordinary character (p. 71):

$$\chi_\rho(s)^* = \widetilde{\zeta}_1^{-1} + \cdots + \widetilde{\zeta}_n^{-1} \in \mathfrak{o}.$$

Let $\mathbb{Q}'$ be the prime subfield of $\widetilde{K}$ and $\mathbb{Q}'(\zeta')$ any cyclotomic subfield of $\widetilde{K}$ containing $\widetilde{\zeta}_1, \ldots, \widetilde{\zeta}_n$. Then under any imbedding $\varphi : \mathbb{Q}'(\zeta') \to \mathbb{C}$, it is clear that

[11] A full treatment of Brauer characters can be found in §17B, p. 419*ff*, [19] or in ch. 18, p. 147*ff*, [68].

$\varphi(\chi_\rho(s)^*) = (\varphi(\chi_\rho(s))^*$ where * on the right side really *is* complex conjugation. Thus if $\chi_\rho(s)^* = \chi_\rho(s)$, its image under any imbedding $\mathbb{Q}'(\zeta') \to \mathbb{C}$ is contained in $\mathbb{R}$, and we accordingly say that $\chi_\rho(s)$ is *real*.

Let σ be an automorphism of K – for example an involution $^-$ – then $\chi_\rho(s)^\sigma$ is defined as follows: Express $\rho(s)$ as a matrix in $\mathrm{M}(n,K)$ with respect to some basis of V, and apply σ to its entries; then the eigenvalues $\eta_1, \dots, \eta_n$ of the transformed matrix are again m^{th} roots of unity and do not depend on the basis chosen; we define $\chi_\rho(s)^\sigma$ to be the sum of their lifts $\widetilde{\eta}_1, \dots, \widetilde{\eta}_n$ to K.

The following is a basic theorem of Brauer (Corollary 17.10, p. 424, [19]):

Theorem 1.7.3 *Two completely reducible representations of G over K are equivalent if and only if their Brauer characters*[12] *are equal.* □

When the characteristic of K does not divide g, then of course *every* representation of G is completely reducible by Maschke's Theorem.

Suppose for the rest of this section that the characteristic of K does not divide the order g of G, and let ρ and ρ' be representations which are *absolutely irreducible* – this means that they are irreducible over *every* extension L/K, and is equivalent to being irreducible over an algebraic closure of K. Choose bases for their vector spaces and consider the corresponding matrix representations:

$$\mathsf{P}(s) = (\alpha(s)_{ij}), \quad \mathsf{P}'(s) = (\beta(s)_{kl}), \quad \text{for all } s \in G.$$

If ρ and ρ' are not equivalent, then according to p. 14, [68],

$$\sum_{s\in G} \alpha(s)_{ij}\beta(s^{-1})_{kl} = 0 \quad \text{for any } i,j,k,l, \tag{1.54}$$

while if they are equivalent, we assume they are actually equal and then

$$\sum_{s\in G} \alpha(s)_{ij}\,\alpha(s^{-1})_{kl} = \begin{cases} g/n & \text{if } i = l \text{ and } j = k, \\ 0 & \text{otherwise,} \end{cases} \tag{1.55}$$

since the degree of ρ is not divisible by the characteristic of K (Cor. 1.2.2, p. 16).

If φ and ψ are complex valued functions on G, define

$$(\varphi|\psi) = \tfrac{1}{g}\sum_{s\in G} \varphi(s)\psi(s)^*.$$

This is a nonsingular positive definite Hermitian form on the complex vector space $\mathbb{C}^G$ of dimension g. Now suppose that χ and χ' are the characters of *absolutely* irreducible representations ρ and ρ'. Then the *(first) orthogonality relations* are

$$(\chi|\chi') = \begin{cases} 1 & \text{if } \rho \text{ and } \rho' \text{ are equivalent,} \\ 0 & \text{otherwise.} \end{cases} \tag{1.56}$$

In fact if $\mathbf{H}$ is the subspace of $\mathbb{C}^G$ of class functions and if K is a *splitting field* of G – that is to say all K-irreducible representations over K are actually absolutely irreducible – the characters of the K-irreducible representations form an orthonormal basis of $\mathbf{H}$. Thus the number of absolutely irreducible representations of G is the class number of G. By another theorem of Brauer, a field K of characteristic 0 *is* a splitting field if K contains the m^{th} roots of unity, where m is the *exponent* of G – the smallest positive integer m such that $s^m = 1$ for all $s \in G$.

[12] Defined using the same p-modular system.

In particular χ is the character of an absolutely irreducible representation if and only if $(\chi|\chi) = 1$.

1.7.3 The twisted contragredient representation. Let $\rho : G \to \mathbf{GL}(V)$ be a representation. Since V is a left KG-module (via ρ), $V^* = \mathrm{Hom}_K(V, K)$ is a *right* KG-module determined by

$$\langle v, xa\rangle = \langle av, x\rangle.$$

Now twist the action of KG on V^* via the standard $(K, {}^-)$-involution ${}^-$ on KG to make it into a *left* KG-module $\overline{V^*}$: thus, if we write $\bar{x}$ for $x \in V^*$ when it is considered as an element of $\overline{V^*}$,

$$\langle v, a\bar{x}\rangle = \langle v, x\bar{a}\rangle = \langle \bar{a}v, x\rangle.$$

If $\bar{\rho}^*$ denotes the representation thus afforded by $\overline{V^*}$,

$$\langle v, \bar{\rho}^*(s)\bar{x}\rangle = \langle v, s\bar{x}\rangle = \langle s^{-1}v, x\rangle = \langle \rho(s^{-1})v, x\rangle. \tag{1.57}$$

If ${}^-$ is the identity on K, this means that $\bar{\rho}^*(s) = \rho(s^{-1})^t$. This is the "usual" definition of the contragredient representation.

Suppose ${}^-$ is *not* necessarily the identity on K. In order to calculate the matrix of $\bar{\rho}^*$, the action of K on $\overline{V^*}$ must agree with that implicit in the action of KG, so $\alpha x = x\bar{\alpha}$ where the right side represents the "usual" action of $\bar{\alpha} \in K$ on V^*. Let $\{v_i\}$ be a K-basis of V and $\{x_i\}$ the dual basis of V^*. Then if $\rho(s^{-1})v_j = \sum_i \alpha_{ij}v_i$ and $\bar{\rho}^*(s)x_k = \sum_l \beta_{lk}x_l$ $(\alpha_{ij}, \beta_{ij} \in K)$,

$$\begin{aligned} \langle \rho(s^{-1})v_j, x_k\rangle &= \alpha_{kj} \\ &= \langle v_j,\ \bar{\rho}^*(s)x_k\rangle = \langle v_j, \sum_l \beta_{lk}x_l\rangle = \langle v_j, \sum_l x_l\bar{\beta}_{lk}\rangle \\ &= \bar{\beta}_{jk}. \end{aligned}$$

Thus

$$\mathrm{mat}\,\bar{\rho}^*(s) = (\mathrm{mat}\,\rho(s^{-1}))^{t-}.$$

The representation $\bar{\rho}^* : G \to \mathbf{GL}(\overline{V^*})$ is called the *twisted contragredient* representation of ρ. If χ_ρ is the character of ρ, then the character of $\bar{\rho}^*$ is

$$\chi_{\bar{\rho}^*}(s) = \overline{\chi_\rho(s)^*}, \tag{1.58}$$

where $\chi_\rho(s)^*$ is the "complex conjugate" of $\chi_\rho(s)$ (cf. p. 71).

Now suppose that $\varphi : V \to \overline{V^*}$ is a KG-homomorphism. Define

$$f : V \times V \to K \quad \text{by} \quad f(u, v) = \langle u, \varphi v\rangle.$$

Then f is a sesquilinear form over $(K, {}^-)$ – note in particular that

$$f(u, \alpha v) = \langle u, \varphi(\alpha v)\rangle = \langle u, \alpha\varphi(v)\rangle = \langle u, \varphi(v)\bar{\alpha}\rangle = f(u, v)\bar{\alpha}$$

since $\varphi(v) \in \overline{V^*}$. Its right adjoint is $f_r = \varphi$, so f is nonsingular if and only if φ is an isomorphism. Furthermore if $s \in G$,

$$f(su, sv) = \langle su, \varphi(sv)\rangle = \langle su, s\varphi(v)\rangle = \langle s^{-1}su, \varphi(v)\rangle = \langle u, \varphi(v)\rangle = f(u, v),$$

so that f is *G-invariant.* Conversely much the same computation shows that if f is a G-invariant sesquilinear form on V, then f_r is a KG-homomorphism $V \to \overline{V^*}$.

Theorem 1.7.4 *Let ρ be a representation of G over K. Then ρ is equivalent to its twisted contragredient $\bar{\rho}^*$ if and only if there is a nonsingular G-invariant sesquilinear form over $(K, ^-)$ on the space V of ρ.*

More precisely the G-invariant sesquilinear forms on V correspond bijectively to the KG-homomorphisms $V \to \overline{V^*}$ via $f \rightsquigarrow f_r$, with nonsingular forms corresponding to isomorphisms. □

We now consider what happens to the contragredient under restriction of the scalars. Let$(L, ^-)/(K, ^-)$ be a finite separable extension of fields with involution, and let $\mathrm{Tr} = \mathrm{Tr}_{L/K}$ be the trace in L/K – it is $\neq 0$ since L/K is separable. Let V be a finite dimensional vector space over L, and denote by V_K the vector space V viewed as a vector space over K. Let $V^* = \mathrm{Hom}_L(V, L)$ and $(V_K)^* = \mathrm{Hom}_K(V_K, K)$. Then the map

$$\tau : (V^*)_K \to (V_K)^*, \quad \tau(x) = \mathrm{Tr} \circ x,$$

is an isomorphism of K-vector spaces. It suffices to show it is injective, and that is clear since if $x \in V^*$, $x \neq 0$, we choose $v \in V$ such that $x(v) \neq 0$, and then for some $\lambda \in L$, $\mathrm{Tr}(x(\lambda v)) = \mathrm{Tr}(\lambda x(v)) \neq 0$. (The isomorphism also follows from Th. 1.2.10, p. 9.)

Let $\langle\, \cdot\, , \cdot \rangle_L$ denote the pairing between V and V^* and $\langle\, \cdot\, , \cdot \rangle_K$ that between V_K and $(V_K)^*$, and let the L-representation $\rho : G \to \mathbf{GL}(V)$ be denoted by ρ_K when considered as a K-representation $G \to \mathbf{GL}(V_K)$, with twisted contragredients $\bar{\rho}^* : G \to \mathbf{GL}(\overline{V^*})$ and $\bar{\rho}^*_K : G \to \mathbf{GL}(\overline{(V_K)^*})$ respectively. If $v \in V$, $x \in \overline{V^*}$ and $s \in G$,

$$\begin{aligned} \langle v, \bar{\rho}^*_K(s)\tau(x)\rangle_K &= \langle \rho_K(s^{-1})v, \tau(x)\rangle_K \\ &= \mathrm{Tr}\langle \rho(s^{-1})v, x\rangle_L = \mathrm{Tr}\langle v, \bar{\rho}^*(s)x\rangle_L \\ &= \langle v, \tau(\bar{\rho}^*(s)x)\rangle_K. \end{aligned}$$

Thus $\bar{\rho}^*_K(s)\tau(x) = \tau(\bar{\rho}^*(s)x)$ for all $x \in V^*$ and $s \in G$, so

Theorem 1.7.5 *The canonical K-isomorphism $\tau : \overline{(V^*)_K} \to \overline{(V_K)^*}$ establishes an equivalence between the representation $\bar{\rho}^*$ of G on $\overline{V^*}$, considered as K-space $(\overline{V^*})_K$, and the representation $\bar{\rho}^*_K$ of G on the space $\overline{(V_K)^*}$.* □

To put it another way, if we identify $(V^*)_K$ and $(V_K)^*$ via τ, the twisted contragredient of ρ as an L-representation, when considered as a K-representation, is the same as the twisted contragredient of ρ considered as a K-representation.

Exercise. If U and V are finite dimensional K-spaces, there is a canonical isomorphism

$$\varphi : U^* \otimes_K V^* \to (U \otimes_K V)^*$$

determined by

$$\langle u \otimes v, \varphi(u^* \otimes v^*)\rangle = \langle u, u^*\rangle\langle v, v^*\rangle.$$

Suppose that U and V are KG-modules. Then $\overline{U^*}$ and $\overline{V^*}$ are (left) KG-modules, and so therefore is $\overline{U^*} \otimes_K \overline{V^*}$ (p. 70). Also $U \otimes_K V$ is a KG-module, and so its twisted contragredient $\overline{(U \otimes_K V)^*}$ is also. Show that

$$\bar{\varphi} : \overline{U^*} \otimes_K \overline{V^*} \to \overline{(U \otimes_K V)^*},$$

defined in the obvious way, is a KG-isomorphism. □

1.7.4 Induced representations. References are §3.3, pp. 28*ff*, [68] and §43, pp. 314*ff*, [18]). See also pp. 161*ff* later in this book.

Let H be a subgroup of the finite group G, and let W be a (finite dimensional) KH-module, affording the representation σ of H. If we view KG as a (KG, KH)-bimodule, the tensor product

$$V = \mathrm{Ind}_H^G W = KG \otimes_{KH} W$$

is a KG-module; the representation of G it affords, the *representation induced from* σ, is denoted by $\mathrm{Ind}_H^G \sigma$. Since V is the vector space direct sum of the $s \otimes W$ as $s \in G$ runs over a system of (left coset) representatives of G/H, the dimension of V is $[G:H] \dim W$.

When there is no danger of confusion, we write $\mathrm{Ind}\, W$ for $\mathrm{Ind}_H^G W$ and $\mathrm{Ind}\,\sigma$ for $\mathrm{Ind}_H^G \sigma$.

Induction of representations is transitive in the sense that if G is in turn a subgroup of a finite group F, then

$$\mathrm{Ind}_G^F(\mathrm{Ind}_H^G W) \cong \mathrm{Ind}_H^F W \quad (\text{ isomorphism of } KF\text{-modules}).$$

One can also start with a representation $\rho : G \to \mathbf{GL}(V)$ of G, and restrict it to a representation $\rho|_H : H \to \mathbf{GL}(V)$ of H. This representation is denoted by $\mathrm{Res}_H^G\, \rho$ or simply $\mathrm{Res}\, \rho$, and its space (which is V of course) by $\mathrm{Res}_H^G V$ or $\mathrm{Res}\, V$.

Now suppose that $\rho : G \to \mathbf{GL}(V)$ and $\sigma : H \to \mathbf{GL}(W)$ are representations. Then there is a KG-isomorphism

$$\varphi : \mathrm{Ind}(W \otimes_K \mathrm{Res}\, V) \to (\mathrm{Ind}\, W) \otimes_K V, \tag{1.59}$$

usually referred to as "Frobenius Reciprocity". Thus φ is an isomorphism

$$\varphi : KG \otimes_{KH} (W \otimes_K \mathrm{Res}\, V) \to (KG \otimes_{KH} W) \otimes_K V, \tag{1.60}$$

and we shall show that φ can be chosen as

$$\varphi((\sum_s \alpha_s s) \otimes (w \otimes v)) = \sum_s \alpha_s((s \otimes w) \otimes sv). \tag{1.61}$$

First note that the map

$$KG \times W \times \mathrm{Res}\, V \to (KG \otimes_{KH} W) \otimes_K V, \quad (\sum_s \alpha_s s, w, v) \to \sum_s \alpha_s((s \otimes w) \otimes sv)$$

is K-trilinear, and so the map

$$KG \times (W \otimes_K V) \to (KG \otimes_{KH} W) \otimes_K V$$

determined by

$$(\sum_s \alpha_s s, w \otimes v) \to \sum_s \alpha_s((s \otimes w) \otimes sv)$$

is K-bilinear. This map is balanced with respect to KH – where $h \in H$ operates on $W \otimes_K V$ via $w \otimes v \to hw \otimes hv$ – and so the map φ in (1.61) is well-defined. Moreover it is a KG-homomorphism since $\varphi(sx) = s\varphi(x)$ for all s and x.

To show that it is an isomorphism, we construct the inverse homomorphism ψ. Consider the map

$$\begin{aligned} &KG \times W \times V \to KG \otimes_{KH} (W \otimes_K \mathrm{Res} V) \\ &(\sum_s \alpha_s s, w, v) \to \sum_s \big(\alpha_s s \otimes_{KH} (w \otimes_K s^{-1} v)\big). \end{aligned}$$

It is K-trilinear and the triples $(\sum_s \alpha_s sh, w, v)$ and $(\sum_s \alpha_s s, hw, v)$ have the same image, and so gives a K-linear map

$$(KG \otimes_{KH} W) \otimes_K V \to KG \otimes_{KH} (W \otimes_K \operatorname{Res} V)$$

which is the inverse of φ. □

In terms of representations, Frobenius Reciprocity is

$$\operatorname{Ind}_H^G(\sigma \otimes \rho|_H) \cong \operatorname{Ind}_H^G(\sigma) \otimes \rho.$$

1.7.5 Simple components of KG and irreducible representations. Reference: §70, pp. 463*ff*, [18]

Since the characteristic of K does not divide the order g of G, the group algebra KG is separable over K by Maschke's Theorem (p. 70) and so is a direct sum of simple separable K-algebras

$$KG = A_1 \oplus A_2 \oplus \cdots \oplus A_h.$$

Each simple component A_i corresponds to a uniquely determined equivalence class of K-irreducible representations: if $\rho : G \to \mathbf{GL}(V)$ is an irreducible representation, then there is a unique i, $1 \le i \le h$, such that A_i acts faithfully on the KG-module V (cf. p. 69) and ρ is given by

$$G \xrightarrow{\text{incl}} KG \xrightarrow{\text{proj}} A_i \to \operatorname{End}_K V,$$

and $A_j V = 0$ for all $j \neq i$. Conversely if V is a simple A_i-module, this sequence yields a K-irreducible representation. By Ths. 1.2.5 and 1.2.6 (p. 8), A_i is isomorphic to a matrix algebra $\mathrm{M}(n_i, D_i)$ for some K-division algebra D_i, and V is the unique (up to isomorphism) simple A_i-module and is isomorphic to the A_i-module of column vectors $D_i^{n_i \times 1}$. If we identify $A_i = \rho(KG) \subset \operatorname{End}_K V$, then $A_i = \operatorname{End}_{D_i} V$ where $D_i = \operatorname{End}_{KG} V = \operatorname{End}_{A_i} V$ (with D_i acting on the right of V). We let $\rho_i : G \to \mathbf{GL}(V_i)$ be the irreducible representation which corresponds in this way to A_i.

There is a finite separable extension L/K in which ρ_i splits into absolutely irreducible representations. If char $K = 0$, we know by Brauer's theorem (p. 73) that if m is the exponent of G, the field L obtained by adjoining the m^{th} roots of unity to K is such a splitting field for *any* representation of G.

The index $d_i = \sqrt{\dim_{\mathrm{Z}(D_i)} D_i}$ of D_i (or A_i) is significant from a representation-theoretic point of view: if we extend the K-representation ρ_i to the algebraic closure $\widetilde{K}$ of K (or to any splitting field of G), it will in general no longer be irreducible, but the $\widetilde{K}G$-module $V_i^{\widetilde{K}}$ (which affords $\rho_i^{\widetilde{K}}$ over $\widetilde{K}$) splits into a direct sum of simple modules over $A_i^{\widetilde{K}}$, in such a way that the multiplicity (of the isomorphism class) of each simple module in the direct sum is exactly d_i. Furthermore the number of distinct isomorphism classes in this splitting of $V_i^{\widetilde{K}}$ is $z_i = (\mathrm{Z}(D_i) : K)$.

In particular ρ_i is absolutely irreducible (or "split") over K if and only if $d_i = z_i = 1$, which means that $A_i \cong \mathrm{M}(n_i, K)$, i.e. A_i is split. More generally we say that a (possibly reducible) representation is split (over K) if it is the direct sum of absolutely irreducible representations. This is the same as saying that if V is the space of the representation, then the simple summands A_i such that $A_i V \neq 0$ are full matrix algebras $\mathrm{M}(n_i, K)$ over K.

The algebra A_i (or the representation ρ_i) is called "quasisplit" if d_i (but not necessarily z_i) is $= 1$. This means that $A_i \cong \mathrm{M}(n_i, L_i)$ where $L_i = \mathrm{Z}(A_i)$.

Theorem 1.7.6 *Suppose that A is a simple direct summand of KG. If the characteristic of K is $\neq 0$, A is quasisplit.*

Suppose the characteristic is 0 *and that $\bar{A} = A$ where $^-$ is the standard* (K, id)-*involution of KG. Then if $(A, {}^-)$ is symplectic or orthogonal, either A is quasisplit or A is similar (over its center) to a quaternion algebra.*

Let Q be the prime subfield of K, and identify $KG = K \otimes_Q QG$. Let A_1 be the direct summand of QG such that A is a direct summand of $K \otimes_Q A_1 = KA_1 \subset KG$. Suppose first that $\operatorname{char} K \neq 0$. By Ex. 3, p. 17, A_1 is quasisplit, say $A_1 \cong \mathrm{M}(n, L_1)$ where L_1/Q is a finite field extension. Now by the exercise on p. 14, $K \otimes_Q L_1 \cong K_1 \oplus \cdots \oplus K_l$ for fields $K_1, \ldots, K_l$, and so

$$K \otimes_Q A_1 \cong (K \otimes_Q L_1) \otimes_{L_1} A_1 \cong \big(K_1 \otimes_{L_1} A_1\big) \oplus \cdots \oplus \big(K_l \otimes_{L_1} A_1\big), \qquad (1.62)$$

and since one of these summands is A, the first statement follows. This argument also shows that, in the case of characteristic 0 (which we now assume), A is quasisplit if A_1 is quasisplit.

Assume A is not quasisplit. Since $\bar{A} = A$ and the involution is the identity on the center of A, A is isomorphic to its opposite algebra and so has order 2 in the Brauer group (over its center). Since A is one of the summands in (1.62), A_1 is not quasisplit either and furthermore $\bar{A}_1 = A_1$. So it has order 2 in the Brauer group of its center which, as a finite extension of $Q = \mathbb{Q}$, is a global field. Thus A_1 is similar to a quaternion algebra (p. 19) and so therefore is A. □

We note that the degree (cf. p. 68) of the irreducible representation ρ_i over K corresponding to $A_i \cong \mathrm{M}(n_i, D_i)$ is $\dim_K D_i^{n_i \times 1} = n_i z_i d_i^2$, while the degree (cf. p. 12) of the K-algebra A_i is $n_i d_i$, which is the degree of any irreducible component of $\rho_i^{\widetilde{K}}$.

An arbitrary linear representation over K is said to be *of odd type* (with respect to $(K, {}^-)$) if $AV = 0$ for each simple summand A of KG which is stable under the standard $(K, {}^-)$-involution of KG and has *even* degree.

Suppose that the characteristic of K is 0, and that G has a normal Abelian subgroup H. By the corollary on p. 61 in [68], the degrees of all irreducible representations of G over an algebraic closure $\hat{K}$ of K divide $[G : H]$. Thus if G has such a subgroup H of odd index – e.g. if the order of G is odd – the degrees of the simple algebra components of $\hat{K}G$ are all odd. Since these degrees are identical with the degrees of the simple algebra components of KG (cf. p. 13), the latter are odd as well. Thus the representations of G over K are all of odd type (if G has a normal Abelian subgroup of odd index and $\operatorname{char} K = 0$).

In general, since the characteristic of K does not divide the degree $d_i n_i$ of A_i (Cor. 1.2.2, p. 16), the center $L_i = \mathrm{Z}(D_i)$ is generated over K by the character values of any character of a representation which is an irreducible constituent of ρ_i over an algebraic closure (cf. (70.8), p. 468, [18]). Since character values are sums of roots of unity, this means that L_i/K is an Abelian extension, i.e. a Galois extension with Abelian Galois group. In fact the character values are sums of m^{th} roots of unity where m is the exponent of G, so L_i is a subfield of the cyclotomic extension of K generated by the m^{th} roots of unity.

We need to generalize these facts slightly:

Lemma 1.7.1 *If A is a simple direct summand of KG then L/K_0 is Abelian.*

We may suppose that $K \neq K_0$. There is a simple direct summand A_1 of K_0G such that A is a direct summand of $K \otimes_{K_0} A_1$. The center L_1 of A_1 is an Abelian extension of K_0, and $K \otimes_{K_0} L_1$ is the center of $K \otimes_{K_0} A_1$.

$$\begin{tikzcd}
& KG \arrow[dl, dash] \arrow[dr, dash] & & & \\
K_0G \arrow[dr, dash] & & K \otimes_{K_0} A_1 \arrow[dl, dash] \arrow[dr, dash] & & \\
& A_1 \arrow[dr, dash] & & K \otimes_{K_0} L_1 \arrow[dl, dash] \arrow[dr, dash] & \\
& & L_1 \arrow[dr, dash] & & K \arrow[dl, dash] \\
& & & K_0 &
\end{tikzcd}$$

Since K/K_0 is a separable extension, $K \otimes_{K_0} L_1$ is a separable L_1-algebra and so is either a separable quadratic extension of L_1 or is $\cong L_1 \oplus L_1$.

In the first case, $K \otimes_{K_0} A_1$ is a simple algebra, so $= A$ and $K \otimes_{K_0} L_1 = L$. Thus L is the compositum of two Abelian extensions of K_0 and so is Abelian over K_0 – it is elementary that the Galois group of L/K_0 is the product of the Galois groups of K/K_0 and L_1/K_0 or one can apply Cor. 1.2.6, p. 22. In the second case,

$$K \otimes_{K_0} A_1 \cong (K \otimes_{K_0} L_1) \otimes_{L_1} A_1 \cong (L_1 \oplus L_1) \otimes_{L_1} A_1 \cong A_1 \oplus A_1.$$

These two copies of A_1 are K-algebras via the two implicit maps $K \to L_1$, but are not in general isomorphic as K-algebras. In any case A must be isomorphic to one of them, and so $L = L_1$ is Abelian over K_0. □

It is often useful to view the process of going up from K to a splitting field $\hat{K}$ of the representation ρ_i – e.g. to an algebraic closure $\widetilde{K}$ – as occurring in two stages: from K to $L_i = \mathrm{Z}(D_i)$, and then from L_i to $\hat{K}$. In the first stage ρ_i splits into its “conjugate representations”. They are most easily understood from the point of view of matrix representations: if the matrix version of one of the L_i-irreducible components of $\rho_i^{L_i}$ is P_{ij} with character χ_{ij}, then the other irreducible components are the $(L_i : K)$ irreducible and mutually inequivalent representations $s \to (\mathsf{P}_{ij}(s))^\sigma$, one for each $\sigma \in \mathrm{Gal}(L_i/K)$. The character of this conjugate representation is simply χ_{ij}^σ, that is to say $s \to \chi_{ij}(s)^\sigma$. Then in the second stage, going from L_i to $\hat{K}$, each of these conjugate representations splits into d_i mutually equivalent absolutely irreducible representations. In the context of representation theory, the index d_i is often referred to as the “Schur index” of the absolutely irreducible representation or character belonging to $\rho_i^{L_i}$ or any of its conjugates (or to ρ_i itself).

1.7.6 Representations over the real and complex numbers. Reference: 13.2, pp. 106*ff*, [68].

Theorem 1.7.7 *(Frobenius–Schur). Let $\rho : G \to \mathbf{GL}(V)$ be a linear representation over the complex numbers $\mathbb{C}$ with character χ. In order that χ have values in $\mathbb{R}$ (resp. that ρ be realizable over $\mathbb{R}$), it is necessary and sufficient that V have a nonsingular bilinear form (resp. nonsingular symmetric bilinear form) invariant under G.* □

A slightly more general version of this theorem, when $\mathbb{C}$ is replaced by the algebraic closure of a real closed field, is given later (Theorem 4.5.4, p. 176).

Assume now that ρ is an irreducible representation over $\mathbb{C}$ of degree $\dim_{\mathbb{C}} V = n$. So the corresponding simple component of $\mathbb{C}G$ is (isomorphic to) $\mathrm{M}(n, \mathbb{C})$. There is a unique (up to equivalence) irreducible representation ρ_0 over $\mathbb{R}$ from which ρ arises by scalar extension from $\mathbb{R}$ to $\mathbb{C}$ – ρ is either $= \rho_0^{\mathbb{C}}$ or is an irreducible component of it.

There are three possible cases:

(a) At least one value $\chi(s)$, $s \in G$, is not real. Then $\rho_0^{\mathbb{C}} = \rho \oplus \rho^*$ where ρ^* is the conjugate representation and is not equivalent to ρ – in terms of the corresponding matrix representation, $\mathsf{P}^*(s) = \mathsf{P}(s)^*$ for all $s \in G$. The character of ρ_0 is $\chi + \chi^*$ and the corresponding simple summand of $\mathbb{R}G$ is $\mathrm{M}(n, \mathbb{C})$. In this case V has no G-invariant nonsingular bilinear form, and ρ is called a *type* 0 representation, or a representation of *unitary type.*[13]

(b) If ρ can be realized over $\mathbb{R}$ – in particular all values of χ are real – ρ is a *type* 1 representation or is *of orthogonal type*. This means that $\rho = \rho_0^{\mathbb{C}}$. The character of ρ_0 is χ and the corresponding simple summand of $\mathbb{R}G$ is $\mathrm{M}(n, \mathbb{R})$. Such a representation ρ has a nonsingular invariant bilinear form which is unique up to a nonzero scalar multiple; the form is symmetric. (See Th. 1.7.8 below).

(c) ρ is a *type* -1 representation or is of *symplectic type* if the values of χ are real but ρ is not realizable over $\mathbb{R}$. In this case $\rho_0^{\mathbb{C}} = \rho \oplus \rho$ and the character of ρ_0 is 2χ. The corresponding direct summand of $\mathbb{R}G$ is $\mathrm{M}(\frac{n}{2}, \mathbb{H})$ where $\mathbb{H}$ is the Hamiltonian quaternion algebra $(-1, -1)_{\mathbb{R}}$. In this case there is again a nonsingular invariant bilinear form which is unique up to a nonzero scalar multiple, but this time it is skew symmetric. (See Th. 1.7.8 below).

This trichotomy is verified in Corollary 4.5.2 (p. 175) for a formally real field $\mathbf{R}$ and its algebraic closure $\mathbf{C} = \mathbf{R}(i)$. In fact it holds in the following form for an arbitrary field K of characteristic 0:

Theorem 1.7.8 *Let $\rho : G \to \mathbf{GL}(V)$ be an irreducible representation over an arbitrary field K of characteristic 0, with character χ, and suppose that A is the simple summand of KG such that $AV \neq 0$. If $h : V \times V \to (K, ^-)$ is a nonzero invariant sesquilinear form, it is nonsingular and, if ρ is absolutely irreducible, is unique up to a scalar.*

Now suppose ρ is absolutely irreducible. Then the "Frobenius-Schur indicator"

$$\frac{1}{|G|} \sum_{s \in G} \chi(s^2) \;=\; 0,\; \pm 1. \tag{1.63}$$

[13] Our terminology is a little unorthodox here – a type 0 representation is often called type 1 in the literature, a type 1 is called a type 2, and a type −1 is called a type 3.

Moreover if $^-$ *is the standard* (K, id)*-involution on* KG,

(a) ρ *has a nonzero invariant bilinear form if and only if the indicator is* $\neq 0$, *and in this case* $\bar{A} = A$.

(b) *If the indicator is* 1, *the unique invariant nonzero bilinear form is a nonsingular symmetric form and* $(A, ^-)$ *is orthogonal.*

(c) *If the indicator is* -1, *the unique invariant nonzero bilinear form is a nonsingular skew symmetric form and* $(A, ^-)$ *is symplectic.*

Suppose $h : V \times V \to K$ is a nonzero G-invariant sesquilinear form. If $u \in \ker h_r = \{u \in V : \ h(V, u) = 0\}$, then for all $s \in G$

$$h(V, su) = h(sV, su) = h(V, u) = 0,$$

so $\ker h_r$ is a proper invariant subspace of V and therefore $= 0$. Thus h is nonsingular, and h_r is a KG-isomorphism (Th. 1.7.4, p. 75). If ρ is absolutely irreducible and h' is another G-invariant sesquilinear form, then $h_r^{-1} h'_r \in \mathrm{End}_{KG} V = K$, so h' is a scalar multiple of h.

Now suppose that ρ is absolutely irreducible – so $A \cong \mathrm{M}(n, K)$ – and let χ be its character. View ρ as a matrix representation $\mathsf{P} : G \to \mathbf{GL}(n, K)$ by choosing a basis of V. Then $\mathsf{P}G \subset \mathbf{GL}(n, K')$ for some subfield K' of K which is finitely generated over the prime subfield and is therefore isomorphic to a subfield K'' of $\mathbb{C}$ – say $\varphi : K' \to K''$. We denote by $\mathsf{P}^{K''}$ the matrix representation over K'' obtained from P via φ, by X $(= \varphi\chi)$ its character, and by $\mathsf{P}^{\mathbb{C}}$ this representation viewed as a representation over $\mathbb{C}$ and $\mathsf{X}^{\mathbb{C}} = \mathsf{X}$ its character. By Prop. 39, p. 109, [68], the relation (1.63) holds over $\mathbb{C}$ (with χ replaced by $\mathsf{X}^{\mathbb{C}}$ of course).

Since $\varphi\chi = \mathsf{X}^{\mathbb{C}}$, we immediately get (1.63).

Suppose that the indicator is -1, for example. By Props. 38 and 39, [68], there is a nonsingular invariant skew symmetric form f, which we view as a polynomial over $\mathbb{C}$ in the $2n$ indeterminates $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{y} = (y_1, \ldots, y_n)$. Let $\{\omega_i\}$ be a basis of $\mathbb{C}$ over K'', and write,

$$f(\vec{x}, \vec{y}) = \sum_i \omega_i f_i(\vec{x}, \vec{y}), \quad f_i \in K''[\vec{x}, \vec{y}] \text{ for all } i.$$

Then for all $s \in G$

$$\begin{aligned} f(\mathsf{P}^{K''}(s)\vec{x},\ \mathsf{P}^{K''}(s)\vec{y}) &= \sum_i \omega_i f_i(\mathsf{P}^{K''}(s)\vec{x}, \mathsf{P}^{K''}(s)\vec{y}) \\ &= f(\vec{x}, \vec{y}) = \sum_i \omega_i f_i(\vec{x}, \vec{y}), \end{aligned}$$

so $f_i(\mathsf{P}^{K''}(s)\vec{x},\ \mathsf{P}^{K''}(s)\vec{y}) = f_i(\vec{x}, \vec{y})$ for all i and all s, that is to say, the f_i are invariant. Similarly

$$\begin{aligned} f(\vec{x}, \vec{y}) &= \sum_i \omega_i f_i(\vec{x}, \vec{y}) \\ &= -f(\vec{y}, \vec{x}) = \sum_i \omega_i(-f_i(\vec{y}, \vec{x})) \end{aligned}$$

implies that all f_i are skew symmetric. At least one of the f_i is $\neq 0$, say f_j, and so $\varphi^{-1} f_j$ is a nonzero (and so nonsingular) invariant skew symmetric form for P, and so also for ρ. Thus $\mathsf{P} : G \to \mathbf{Sp}(n, K')$ and $\rho : G \to \mathbf{Sp}(n, K)$, and

$(\varphi^{-1}f_j)(au,v) = (\varphi^{-1}f_j)(u,\bar{a}v)$ for all $a \in KG$. This implies that $\bar{A} = A$, and that

$$(A, ^{-}) \xrightarrow{\rho} (\mathrm{End}V, ^{\sim}), \quad \text{(where } ^{\sim} \text{ is the adjoint involution of } \varphi^{-1}f_j\text{)},$$

is an isomorphism. Thus $(A, ^{-})$ is symplectic (Prop. 1.5.1, p. 47).

Similarly if the indicator is 1, there is a nonsingular invariant symmetric form for ρ, and $(A, ^{-})$ is orthogonal.

If the indicator for χ is 0, it is easy to see that the indicator for $\mathsf{X}^{\mathbb{C}}$ is also 0, and so $\mathsf{P}^{\mathbb{C}}$ has no nonzero invariant forms. But if ρ has a nonzero invariant form, an argument similar to the above shows that $\mathsf{P}^{\mathbb{C}}$ must also have one, which is a contradiction. □

If K can be imbedded in $\mathbb{C}$, as is “usually” the case, this theorem is more easily proved by simply replacing K by an imbedding into $\mathbb{C}$.