§2.7. Quaternion Algebras over Number Fields.

k : a number field. v : a valuation on k.

k_v (or k_p in the non-Archimedean case) : the completion of k at v (or p), a local field.

$\Rightarrow$ k embeds in k_v for each v & elements of k are usually identified with their images in k_v.

Def 2.7.1 A : a quaternion alg. over k.
Let A_v (resp. A_p) denote the quaternion algebra $A \otimes_k k_v$ (resp. $A \otimes_k k_p$) over k_v (resp. k_p). Then A is said to be ramified at v (resp. at p) if A_v (resp. A_p) is the unique division algebra over k_v (resp. k_p) (assuming that v is not a complex embedding). Otherwise, A splits at v or p. //

Hasse-Minkowski Thm k : a number field.
(V, B) : a quad. space over k.
Then V is isotropic over k iff V is isotropic over all k_v where v ranges over all places over k. //

Corollary $a \in k^*$. V represents a iff V represents a in all k_v where v ranges over all places of k.

Theorem 2.7.2 A : a quaternion algebra over k.
Then A splits over k iff $A \otimes_k k_v$ splits over k_v for all v.
Pf). Let $A = \left(\frac{a,b}{k}\right)$. $\Rightarrow$ A splits over k iff $ax^2+by^2=1$ has a solution in k. (Thm 2.3.1).
$\Rightarrow$ By the Hasse-Minkowski Thm, $ax^2+by^2=1$ has a sol. in k iff it has a solution in k_v $\forall v$.

And, $ax^2+by^2=1$ has a solution in k_v iff $A\otimes_k k_v$ splits over k_v. ▨

Recall $a,b\in k^*$

$\Rightarrow$ Hilbert symbol $(a,b)=\begin{cases}1 & \text{if } ax^2+by^2 \text{ represents } 1.\\ -1 & \text{otherwise.}\end{cases}$

Hilbert's Reciprocity Law The set of places $\{v \mid (a,b)=-1 \text{ in } k_v\}$ is finite and of even cardinality.

Theorem 2.1.3 # of places v on k s.t. A is ramified at v is of even cardinality. //

Def. 2.1.4 The finite set of places at which A is ramified will be denoted by $\mathrm{Ram}(A)$, the subset of Archimedean ones by $\mathrm{Ram}_\infty(A)$ and the non-Archimedean ones by $\mathrm{Ram}_f(A)$. The places $v\in \mathrm{Ram}_f(A)$ correspond to prime ideals P, and the (reduced) discriminant of A, $\Delta(A)$ is the ideal defined by

$$\Delta(A)=\prod_{P\in \mathrm{Ram}_f(A)} P .$$

Theorem 2.1.5 A, A' : quaternion algebras over k.

$\Rightarrow A\cong A'$ iff $\mathrm{Ram}(A)=\mathrm{Ram}(A')$.

Pf) By Thm 2.3.4, $A\cong A'$ iff A_0, A_0' are isometric.

& By Thm 0.9.12, A_0, A_0' are isometric iff $(A_0)_v, (A_0')_v$ are isometric over k_v $\forall v$.

$\Rightarrow$ Since $(A_0)_v=(A_v)_0$, it follows that $A\cong A'$ iff $A_v\cong A_v'$ for all v.

For each complex Archimedean v, $A_v\cong A_v'$ and for all other v, there are precisely two possibilities by Thm 2.5.1 & Cor. 2.6.4.

$\Rightarrow \mathrm{Ram}(A)=\mathrm{Ram}(A')$ shows that $A_v\cong A_v'$ $\forall v$. ▨

Remark: Quaternion algebras are determined by their ramification sets //

§2.8. Central Simple Algebras.

F: a field. (all module and v.s. actions will be on the right).

Def. 2.8.1 An F-algebra A is a vector space over F, which is a ring with 1 satisfying

$$(ab)x = a(bx) = (ax)b \quad \forall a,b \in A, x \in F.$$

Throughout, all algebras will be finite-dimensional.

If A' is a subalgebra of A, then the centraliser of A'

$$C_A(A') = \{a \in A \mid aa' = a'a \quad \forall a' \in A'\}$$

is also a subalgebra. In particular, the center $Z(A) = C_A(A)$ is a subalgebra. Furthermore, F embeds as $1_A \cdot F$ as a subset of $Z(A)$.

If M is an A-module, then $\mathrm{End}_A(M)$ is the set of A-module endomorphisms $\phi : A \longrightarrow A$. Under composition of mappings, $\mathrm{End}_A(M)$ is also an F-algebra with the identity mapping as 1.

Lemma 2.8.2 The left regular representation λ induces an isomorphism $A \cong \mathrm{End}_A(A)$.

Pf) For $a \in A$, $\lambda_a \in \mathrm{End}_A(A)$ & $\lambda_a(b) = ab \quad \forall b \in A$.

$\Rightarrow \lambda : A \longrightarrow \mathrm{End}_A(A)$, $a \longmapsto \lambda_a$ is an alg. homomorphism.

Since A has an identity element, the kernel of λ is necessarily trivial. ($\because a \in \ker\lambda \Rightarrow \lambda_a$ is the identity map i.e.

$$\Rightarrow \lambda_a(1) = a \cdot 1 = a = 1).$$

So, λ is injective. Further, if $\phi \in \mathrm{End}_A(A)$, then,

$$\phi(a) = \phi(1 \cdot a) = \phi(1)a = \lambda_{\phi(1)}(a).$$

$\Rightarrow \phi = \lambda_{\phi(1)}$ so λ is surjective. ∎

Def. 2.8.3

- An F-algebra A is central if $Z(A) = F$.
- An F-algebra A is simple if it has no proper two-sided ideals.

Note A, B : F-algebras

$\Rightarrow A \otimes_F B$ is also an F-algebra with $\dim_F(A \otimes B) = (\dim_F A)(\dim_F B)$.

Prop. 2.8.4 A, B : F-algebras.

1. If A' and B' are subalgebras of A and B, resp.,
$$C_{(A\otimes B)}(A' \otimes B') = C_A(A') \otimes C_B(B').$$
In particular, if A and B are central, so is $A \otimes B$.
2. If A is central simple and B is simple, then $A \otimes B$ is simple.
In particular, if A and B are central simple, so is $A \otimes B$.

Proof) Let $E = A \otimes B$.

1. In $A \otimes_F B$, $(a \otimes_F b)(a' \otimes_F b') = aa' \otimes_F bb'$.
$\Rightarrow C_A(A') \otimes C_B(B') \subset C_E(A' \otimes B')$.
Choose a basis $\{b_j\}$ of B. Then, if $e \in C_E(A' \otimes B')$, e has a unique expression as $e = \sum \alpha_j \otimes b_j$ with $\alpha_j \in A$.
Let $a' \in A'$. Then from $e(a' \otimes 1) = (a' \otimes 1)e$ and the uniqueness, we obtain $\alpha_j a' = a' \alpha_j$ for each j and all $a' \in A'$.
$\Rightarrow \alpha_j \in C_A(A')$ and so $e \in C_A(A') \otimes B$.
With the similar way, we can see that $e \in A \otimes C_B(B')$.
$\therefore e \in C_A(A') \otimes C_B(B')$. //

2. Let $I \neq 0$ be an ideal of E. Let $0 \neq z \in I$ so that $z = \sum_{i=0}^{r} a_i \otimes b_i$ with $a_i \in A$ and $b_i \in B$ and chosen among elements of I s.t. r is minimal.

Thus all a_i and b_i are non-zero and $\{a_1, \cdots, a_r\}$ is linearly indep. Otherwise, after renumbering, $a_1 = \sum_{i=2}^{r} a_i x_i$ and,

$z = \sum_{i=2}^{r} a_i \otimes (b_1 x_i + b_i)$, contradicting the minimality of r.

In the same way, $\{b_1, \cdots, b_r\}$ is linearly indep.

We now "replace" $\{a_1, \cdots, a_r\}$ by a set $\{1, a_2', \cdots, a_r'\}$. The set Aa_1A is a two-sided ideal and so $Aa_1A = A$. Thus $1 = \sum_j c_j a_1 d_j$.

So, $z_1 = \sum_j (c_j \otimes 1) z (d_j \otimes 1) = 1 \otimes b_1 + \sum_{i=2}^{r} a_i' \otimes b_i \in I$.

Now repeat for b_1 to obtain an element

$$z' = 1 \otimes 1 + \sum_{i=2}^{r} a_i' \otimes b_i' \in I.$$

$$\Rightarrow z'(a \otimes 1) - (a \otimes 1) z' = \sum_{i=2}^{r} (a_i' a - a a_i') \otimes b_i' \in I,$$

$\Rightarrow$ The choice of r shows that $a_i' a = a a_i'$ for $i = 2, 3, \cdots, r$.

$\Rightarrow a_i' \in Z(A) = F$.

However, $\{1, a_2', \cdots, a_r'\}$ is lin. indep. $/F$. So $r = 1$ and $1 \otimes 1 \in I$. Thus $I = E$. ∎

Def 2.8.5 For the F-algebra A, let A° denote the opposite algebra where multiplication $\circ$ is defined by

$$a \circ b = b \cdot a \quad \forall\ a, b \in A.$$

Cor. 2.8.6 If A is a central simple algebra, so is A° and $A \otimes A^\circ \cong \mathrm{End}_F(A)$.

Proof) Obviously, A° is also central & simple.

Define $\theta = A \otimes A^\circ \longrightarrow \mathrm{End}_F(A)$ by $\theta(a \otimes b)(c) = acb$

for $a, b, c \in A$. $\Rightarrow \theta$ defines an alg. homomorphism.

By Prop. 2.8.4, $A \otimes A^\circ$ is simple and so θ is injective.
($\because \ker\theta$ is a two-sided ideal of $A \otimes A^\circ \Rightarrow \ker\theta = 0$).
& $\dim A \otimes A^\circ = (\dim A)^2 = \dim(\mathrm{End}_F(A))$. $\Rightarrow \theta$ is surjective. ///

Brauer group.

On the set of central simple algebras over a field K, define A to be equivalent to B if $\exists\ m, n \in \mathbb{Z}$ s.t.

$$A \otimes M_m(K) \cong B \otimes M_n(K).$$

→ Since $M_m(K) \otimes M_n(K) \cong M_{mn}(K)$ ~ for showing transitivity //
($\because$ $A \otimes B \longmapsto$ the Kronecker product of A, B.
is an isomorphism.).

this is an equivalence relation and we denote the set of equiv. classes by $Br(K)$.

If $[A]$ denotes the equiv. class of A in $Br(K)$, then

$$[A] \cdot [B] = [A \otimes B]$$

is a well-defined binary operation by Prop. 2.8.4.
⇒ This operation is associative and $[K]$ is the identity.
& each element $[A]$ has an inverse $[A^\circ]$ by Cor. 2.8.6.
⇒ $Br(K)$ is an abelian group, the Brauer Group of K.

Remark A: a quaternion algebra $\Rightarrow A \cong A^\circ$.
$\Rightarrow [A]$ has order 2 in $Br(K)$.

Later we will show that the subset of $Br(K)$ of elts rep. by quaternion algebras is a subgp of exponent 2, in the cases where K is a number field.

(↓ the least common multiple of gp elements.) //

§2.9. The Skolem Noether Theorem.

A : an F-algebra, F : a field.

Def. 2.9.1 A right module M over A is simple if it has no proper submodules. It is semi-simple if it is a direct sum of simple modules.

Lemma 2.9.2 (Schur's Lemma) M, N : A-modules.
$\phi : M \to N$ a nonzero homo.
1. If M is simple, ϕ is injective.
2. If N is simple, ϕ is surjective.

Proof) $\ker\phi$, $\mathrm{Im}\,\phi$ are submodules of M, N resp. ▨

Cor. 2.9.3 N: a simple A-module $\to \mathrm{End}_A(N)$ is a division algebra.

Proof) By Schur's lemma, $\phi \in \mathrm{End}_A(N) \Rightarrow \phi$ is bijective. ▨

Note When A is regarded as a right A-module, we denote by A_A.
& A_A is simple if it has no proper right ideal.

Lemma 2.9.4 M: a module s.t. $M = \sum_{j\in J} N_j$, where each N_j is a simple submodule of M. Then if P is any submodule of M, $\exists$ a subset I of J s.t. $M = \oplus\sum_{i\in I} N_i \oplus P$.

Proof) By Zorn's Lemma, $\exists$ a subset I of J s.t. the collection $\{N_i ; i\in I\} \cup \{P\}$ is maximal w.r.t. the property $\sum_{i\in I} N_i + P = \oplus\sum_{i\in I} N_i \oplus P$. Let $M_1 = \oplus\sum_{i\in I} N_i \oplus P$.
$\Rightarrow$ By the maximality of I, $N_j \cap M_1 \neq 0$ for $j \in J$.
$\Rightarrow$ Since N_j is simple and $N_j \cap M_1$ is a submodule of N_j,
$N_j \cap M_1 = N_j \Rightarrow N_j \subset M_1$ $\forall j$. $\therefore M = M_1$ ▨

Prop. 2.9.5 A: a fin.-dim. simple algebra over F.
$\Rightarrow$ the following two conditions hold :

1. A_A is semi-simple.
2. All non-zero minimal right ideals of A are isomorphic.

Pf) 1. Let N be a nonzero minimal right ideal of A.
$\Rightarrow AN = \sum_{x \in A} xN$ is a two-sided ideal of A and so $AN = A$.

Note Each right ideal of an alg. A is an A-module and will be simple A-module iff it is a minimal right ideal.

Since N is minimal, it is a simple A-module.
$\Rightarrow$ By Schur's Lemma, using λ_x, each $xN = \lambda_x(N)$ is either 0 or simple.

Thus A is a sum of simple submodules and taking $P = 0$ in Lemma 2.9.4, A is semi-simple.

2. N_1, N_2 : two nonzero minimal right ideals of A.
$\Rightarrow AN_1 = AN_2 = A$. $\Rightarrow A(N_1N_2) = A$ & $N_1N_2 \neq 0$.
Choose $x_1 \in N_1$ s.t. $x_1N_2 \neq 0$. Since $x_1N_2 \subset N_1$, the minimality of N_1 gives $x_1N_2 = N_1$. Then by Schur's lemma, $\lambda_{x_1} : N_2 \to N_1$ is an isomorphism. ▨

Thm 2.9.6 (Wedderburn's Structure Theorem)
A : a simple algebra of fin. dim. over the field F.
$\Rightarrow A \cong M_n(D)$, where $D \cong \mathrm{End}_A(N)$ is a division algebra with N a minimal right ideal of A.
The integer n and division algebra D are uniquely determined by A.

Proof) By Lemma 2.8.2, $A \cong \mathrm{End}_A(A)$, and by Prop. 2.9.5, A_A is iso. to a direct sum of a number of copies, say n, of a minimal right ideal N. $\Rightarrow A \cong M_n(\mathrm{End}_A(N))$ (see Ex 2.8, No. 1).

& By Cor 2.9.3, $\mathrm{End}_A(N) = D$, a division algebra.

We now establish the uniqueness of n and D.

Supp. $A \cong M_{n'}(D')$ for some division alg. D'. Let ε_i denote the $n' \times n'$ matrix with 1 in entry (i,i) and zeros everywhere.

$\Rightarrow N_i = \varepsilon_i M_{n'}(D')$ is a right ideal and $A = \bigoplus \sum_{i=1}^{n'} N_i$. Since D' is a division algebra, N_i is minimal.

(If $0 \neq M_i \subset N_i \Rightarrow M_i = N_i$)

$\Rightarrow$ By Prop. 2.9.5, $n' = n$. //

For $d' \in D'$, $\lambda_{d'} \in \mathrm{End}_A(N_i)$ and the mapping $d' \longrightarrow \lambda_{d'}$ is an inj. homomorphism.

Now supp. that $\phi \in \mathrm{End}_A(N_i)$ and $\phi(\varepsilon_i) = \varepsilon_i \beta$, $\beta \in M_{n'}(D')$.

Then $\phi(\varepsilon_i) = \phi(\varepsilon_i^2) = \phi(\varepsilon_i)\varepsilon_i = \varepsilon_i \beta \varepsilon_i$.

($\because \varepsilon_i^2 = \varepsilon_i$; ϕ is an A-module homo. (right))

However, $\exists\, d' \in D'$ s.t. $d'\varepsilon_i = \varepsilon_i \beta \varepsilon_i$. (we take $d' = (1,1)$ entry of β).

Now let $\alpha \in N_i$. Then.

$\phi(\alpha) = \phi(\varepsilon_i \alpha) = \phi(\varepsilon_i)\alpha = \varepsilon_i \beta \alpha = \varepsilon_i \beta \varepsilon_i \alpha = d' \varepsilon_i \alpha = d'\alpha$.

($\alpha = \varepsilon_i \beta \Rightarrow \varepsilon_i \alpha = \varepsilon_i^2 \beta = \varepsilon_i \beta = \alpha$)

Thus $\phi = \lambda_{d'} \Rightarrow d' \longrightarrow \lambda_{d'}$ is surj.

$\Rightarrow D' \cong \mathrm{End}_A(N_i) \cong \mathrm{End}_A(N) \cong D$. ▨

($N_i \cong N$).

Prop. 2.9.7 M_1, M_2 : right A-modules.

$\Rightarrow M_1 \cong M_2$ iff $\dim_F(M_1) = \dim_F(M_2)$. //

Theorem 2.9.8 (Skolem Noether Theorem).

A: a fin. dim. central simple algebra / F.

B: a fin. dim. simple algebra / F.

If $\phi, \psi : B \to A$ are alg. homomorphisms, then there exists an invertible element $c \in A$ s.t. $\phi(b) = c^{-1}\psi(b)c$ for all $b \in B$.

Proof) Supp. first that A is a matrix algebra over F.

(i.e. $A = \mathrm{End}_F(V)$ for a vector space V)

$\Rightarrow$ Using ϕ, V becomes a right B°-module V_ϕ, by defining $\alpha b = \phi(b)(\alpha)$ for $\alpha \in V$, $b \in B$. In the same way, we obtain V_ψ. Thus by Prop 2.9.1, V_ϕ and V_ψ are iso. B°-modules.

Let $c : V_\phi \to V_\psi$ be such an iso. so that c is an inv. elt of $A = \mathrm{End}_F(V)$.

Since c is a B°-module iso., $c(\alpha \cdot b) = c(\alpha) \cdot b$ (w.r.t. ϕ on the left, w.r.t. ψ on the right)

$$\Rightarrow c(\phi(b)(\alpha)) = \psi(b)(c(\alpha)) \quad \forall \alpha \in V.$$

$\Rightarrow \phi(b) = c^{-1}\psi(b)c$ for all $b \in B$.

In the general case, consider

$\phi \otimes 1, \psi \otimes 1 : B \otimes A^\circ \to A \otimes A^\circ \cong \mathrm{End}_F(A)$ by Cor. 2.8.6.

Now $B \otimes A^\circ$ is simple by Prop. 2.8.4.

$\Rightarrow$ As above, $\exists\ \bar{c} \in A \otimes A^\circ$ s.t. $\bar{c}^{-1}(\psi(b) \otimes a)\bar{c} = \phi(b) \otimes a$ for all $b \in B$, $a \in A$.

Putting $b = 1$ gives $\bar{c} \in C_{A \otimes A^\circ}(1 \otimes A^\circ) = Z(1) \otimes Z(A^\circ) = A \otimes_F 1$ by Prop. 2.8.4. $\Rightarrow \bar{c} = c \otimes 1$ for some $c \in A$. Similarly, $\bar{c}^{-1} \in A \otimes 1 \Rightarrow c$ is an inv. elt of A. Then putting $a = 1$ above gives $c^{-1}\psi(b)c = \phi(b)$ $\forall b \in B$. ▨

Cor 2.9.9 Every non-zero endomorphism of a fin. dim. central simple algebra is an inner automorphism.

//.