Separability of Algebras

May 26, 2008

Contents

Abstract

This series of lectures intend to give an overview of the notion of separability in algebra. Begining with separable field extensions, we review the theory of finite dimensional central division algebras over a given field via the theory of central simple algebras, the construction of the Brauer group and its representation via crossed products and group cohomology. In the second lecture we will introduce Azumaya algebras and state their basic properties following work of Auslander and Goldman as well as Hirata and Sugano for non-commutative separable ring extensions. In the third lecture we apply the notion of separability to group rings and skew group rings; semisimplicity (Maschke's Theorem) and Von Neumann regularity will be discussed. In the last lecture we will illustrate separability in the context of Hopf algebra actions.

Chapter 1

The Brauer group of a field

The Brauer group describes the finite dimensional division algebras over a given field. In this section K will always denote a field and $\otimes = \otimes_K$.

1.1 Separable field extensions

Let us denote the algebraic closure of a field K by $\overline{K}$.

Definition 1.1 *Let $K \subseteq L$ be a field extension. An element $a \in L$ is called* **separable** *over K if its minimal polynomial* $\mathrm{minpoly}_K(a)$ *has only simple roots, i.e. it is irreducible in $\overline{K}[x]$.*

Definition 1.2 *A field extension $K \subseteq L$ is called* **separable** *if every element of L is separable over K.*

Given two field extensions E and L over K. The question is whether $E \otimes L$ can contain nilpotent elements or whether it is semisimple artinian.

Let a be an algebraic element over K, set $L = K(a)$ and let $f(x) = \mathrm{minpoly}_K(a)$ with $n = \deg(f(x))$. Then $1, a, \cdots, a^{n-1}$ form a basis of $L \simeq K[x]/K[x]f(x)$. Consider the homomorphism

$$\phi : \overline{K} \otimes_K L \longrightarrow \overline{K}[x]/\overline{K}[x]f(x)$$

with $\phi\left(\sum_{i=0}^{n-1} \alpha_i \otimes a^i\right) = \sum_{i=0}^{n-1} \alpha_i \overline{x}^i$ where $\overline{x}$ denotes the image of x under the projection $\overline{K}[x] \to \overline{K}[x]/\overline{K}[x]f(x)$. Since the powers $1, a, a^2, \cdots, a^{n-1}$ form a basis of L, ϕ is well-defined. Since $1, \overline{x}, \cdots, \overline{x}^{n-1}$ are linearly independent, ϕ is injective and hence an isomorphism of K-algebras as $\dim_{\overline{K}}(\overline{K} \otimes L) = \dim_{\overline{K}}(\overline{K}[x]/\overline{K}[x]f(x))$. Over $\overline{K}$, $f(x)$ decomposes into linear factors, let's say

$$f(x) = p_1(x)^{m_1} p_2(x)^{m_2} \cdots p_k x^{m_k}$$

where $\deg(p_i(x)) = 1$ and $m_i \geq 1$. By the chinese remainder theorem we have an isomorphism of algebras:

$$\overline{K} \otimes_K L \simeq \overline{K}[x]/\overline{K}[x]f(x) \simeq \prod_{i=1}^{k} \overline{K}[x]/\overline{K}[x]p_i(x)^{m_i}$$

Note that $\overline{K}[x]/\overline{K}[x]p_i(x)^{m_i}$ is a field if and only if $m_i = 1$. Thus we just proved:

Theorem 1.3 *Let L be a finite dimensional field simple extension of K, i.e. $L = K(a)$. Then L is separable over K if and only if $\overline{K} \otimes_K L$ is semisimple.*

Definition 1.4 *A finite dimensional K-algebra A is* **separable** *over the field K if $A \otimes_K L$ is semisimple for any algebraic field extensions L of K,*

Note that any separable algebra A over K has to be semisimple by choosing $L = K$ in the definition.

1.2 Central simple algebras

Definition 1.5 *Let A be a K-algebra. The center of A is the subring*

$$Z(A) = \{a \in A \mid \forall b \in A : ab = ba\}.$$

The K-algebra A is called **central** *if $Z(A) = K$ and A is called* **simple** *if 0 and A are the only two-sided ideals of A.*

Note that the center of any simple K-algebra A is a field, since any central element $z \in Z(A)$ generates a two-sided ideal Az and therefore $z = 0$ or $Az = A$, i.e. z is invertible in A and thus in $Z(A)$ since inverses of central elements are central.

Compare the next with Theorem 1.3

Theorem 1.6 *Let A be a central simple K-algebra and B a simple K-algebra. Then $A \otimes_K B$ is simple.*

Proof. Any element of $A \otimes B$ can be written as $u = \sum_{i=1}^{n} a_i \otimes b_i$ with non-zero $a_i \in A$ and $b_i \in B$ and the b_i being linearly independent over K. We call n the length of the representation of u.

Let U be a non-zero ideal of $A \otimes B$ and choose an element $0 \neq u \in U$ of mimial length, i.e. $u = \sum_{i=1}^{n} a_i \otimes b_i$ with $0 \neq a_i \in A$, $b_1, \ldots, b_n$ linearly independent and no non-zero element of U has length strictly less than n. Since A is simple and $a_1 \neq 0$, $Aa_1A = A$, i.e. there exist elements $x_1, \ldots, x_m, y_1, \ldots, y_m$ with $\sum_{j=1}^{m} x_j a_1 y_j = 1$. Thus

$$\sum_{j=1}^{m} (x_j \otimes 1)u(y_j \otimes 1) = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} x_j a_i y_j \right) \otimes b_i = 1 \otimes b_1 + \tilde{a}_2 \otimes b_2 + \cdots + \tilde{a}_n \otimes b_n =: \tilde{u}$$

where $\tilde{a}_i = \sum_{j=1}^{m} x_j a_i y_j$. For any $z \in A$:

$$v = (z \otimes 1)\tilde{u} - \tilde{u}(z \otimes 1) = \sum_{i=2} (z\tilde{a}_i - \tilde{a}_i z) \otimes b_i \in U$$

has length less than n. Thus by minimality of n, $v = 0$, i.e. $z\tilde{a}_i = \tilde{a}_i z$ for all i and all $z \in A$. Thus $\tilde{a}_i \in Z(A) = K$. Therefore we can rewrite $\tilde{u}$ as

$$\tilde{u} = 1 \otimes (b_1 + \tilde{a}_2 b_2 + \cdots \tilde{a}_n b_n)$$

Since the b_i's are linearly independent $b := b_1 + \tilde{a}_2 b_2 + \cdots \tilde{a}_n b_n \neq 0$. Thus $B = BbB$ and

$$(A \otimes B)\tilde{u}(1 \otimes B) = (A \otimes 1)(1 \otimes BbB) = A \otimes B.$$

Hence $U = A \otimes B$. ∎

Thus we can conclude

Corollary 1.7 *Any finite dimensional central simple K-algebra is a separable K-algebra.*

Theorem 1.8 *Let A be a finite dimensional central simple K-algebra. Then there exists a finite dimensional central division algebra D over K such that $A \simeq M_n(D)$ and $\dim_K(A)$ is a perfect square*

Proof. Since A is artinian and $\mathrm{Jac}(A) = 0$, by the Wedderburn-Artin theorem A is isomorphic to a finite direct product of matrix rings over division algebras. Since A is simple $A \simeq M_n(D)$ and D is a finite dimensional division algebra over K. Since $K = Z(A) \simeq Z(M_n(D)) \simeq Z(D)$, D is central. Let $\overline{K}$ be the algebraic closure of K. By 1.6 $\overline{D} = D \otimes \overline{K}$ is a simple $\overline{K}$-algebra. Note that $\dim_K(D) = \dim_{\overline{K}}(\overline{D})$. Again by Wedderburn-Artin $D \otimes \overline{K} \simeq M_m(\overline{K})$, i.e. $\dim_K(D) = \dim_{\overline{K}}(\overline{D}) = m^2$ and $\dim_K(A) = (mn)^2$ is a square. ∎

Definition 1.9 *The index of a finite dimensional central simple K-algebra A is defined as* $\mathrm{Ind}_K(A) = \sqrt{\dim_K(A)}$.

Our first application to this observation is the famous

Theorem 1.10 (Skolem-Noether) *Let A and B be finite dimensional simple K-algebras and $\varphi_1, \varphi_2 : A \to B$ non-zero homomorphisms of K-algebras. If B is central, then there exists an invertible element $u \in B$ such that $\varphi_2(a) = u\varphi_1(a)u^{-1}$ for all $a \in A$.*

Proof. As A is simple, φ_i are injective. The K-algebra $A \otimes B^{op}$ is simple and finite dimensional by Theorem 1.6, i.e. $A \otimes B^{op} \simeq M_n(D)$ for some finite dimensional division algebra D and $n \geq 1$. Hence there exists up-to-isomorphism a unique simple $A \otimes B^{op}$-module E with $dim_D(E) = n$. For any finite dimensional $A \otimes B^{op}$-module M we have $M \simeq E^r$ as $A \otimes B^{op}$-modules with $r = dim_D(M)/dim_D(E)$. Thus two $A \otimes B^{op}$-modules are isomorphic if and only if they have the same dimension. Since B is an $B \otimes B^{op}$-module, it is also an $A \otimes B^{op}$-module, defined by

$$(a \otimes b) \cdot x := \varphi_i(a)xb$$

for all $a \in A$, $b, x \in B$ and $i = 1, 2$. Let B_i denote the $A \otimes B$-module structure induced by φ_i for $i = 1, 2$. By the above argument $B_1 \simeq B_2$ as $A \otimes B$-module. Hence there exists a K-linear bijection $f : B = B_1 \to B_2 = B$ such that

$$f(\varphi_1(a)xb) = \varphi_2(a)f(x)b$$

for all $a \in A$ and $x, b \in B$. Hence $f(b) = f(1)b$ for all $b \in B$. Since f is bijective there exists $b \in B$ such that $1 = f(b) = f(1)b$, i.e. $u = f(1)$ is invertible. Thus for all $a \in A$

$$\varphi_2(a)u = 1\varphi_2(a)f(1) = f(\varphi_1(a)) = f(1)\varphi_1(a) = u\varphi_1(a),$$

i.e. $\varphi_2(a) = u\varphi_1(a)u^{-1}$. ∎

Recall that an automorphism $\varphi : R \to R$ of a ring is called **inner** if there exists an invertible element $u \in R$ such that $\varphi(x) = uxu^{-1}$ for all $x \in R$. The Skolem-Noether theorem implies the following

Corollary 1.11 *Every automorphism of a finite dimensional central simple algebra is inner.*

We will now specalise to finite dimensional central simple K-algebras and introduce the Brauer group.

Definition 1.12 *Given two finite dimensional central simple K-algebras A and B we say that A and B are equivalent denoted by $A \sim B$ if there exists $n, m \geq 1$ and an isomorphism*

$$A \otimes_K M_n(K) \simeq B \otimes_K M_m(K)$$

There exists an easier way to see when to finite dimensional central simple K-algebras are equivalent:

Lemma 1.13 *Let $A = M_n(D)$ and $B = M_m(E)$ be two finite dimensional central simple algebras over K with D and E being central division algebras over K. Then $A \sim B$ if and only if $D \simeq E$.*

Proof. If $D \simeq E$, then

$$A \otimes_K M_m(K) \simeq M_n(K) \otimes M_m(K) \simeq M_{nm}(K) \simeq M_m(K) \otimes M_n(K) \simeq B \otimes M_n(K).$$

On the other hand if there are k, l such that

$$M_{nl}(D) \simeq M_n(D) \otimes M_l(K) \simeq A \otimes M_l(K) \simeq B \otimes M_k(K) \simeq M_m(E) \otimes M_k(K) \simeq M_{mk}(E)$$

then any simple $M_{nl}(D)$-module corresponds to a simple $M_{mk}(E)$-module. As any simple module S over $M_{nl}(D)$ is isomorphic to D^{nl} as D-vectorspace it has K-dimension$(nl)dim_K(D)$. Thus $nldim_K(D) = mkdim_K(E)$. On the other hand

$$(nl)^2 dim_K(D) = dim_K(M_{nl}(D)) = dim_K(M_{mk}(E)) = (mk)^2 dim_K(E)$$

which shows that $nl = mk$. Since $D \simeq \mathrm{End}_{M_{nl}(D)}(S)$ for any simple module S, we have $D \simeq E$. ∎

Since any finite dimensional central simple algebra A can be written as $M_n(D)$ we see by the previous Lemma that the relation $\sim$ defines an equivalence relation and that the equivalence classes of finite dimensional central simple K-algebras A, denoted by $[A]$, correspond to the equivalence classes of finite dimensional divison algebras over K.

Definition 1.14 *The* **Brauer group** *of a field K is the set of equivalence classes of finite dimensional central simple K-algebras:*

$$\mathrm{Br}(K) = \{[A] \mid A \text{ is a finite dimensional central simple } K\text{-algebra}\}$$

The next result shows that $\mathrm{Br}(K)$ is closed under tensor product.

Theorem 1.15 *Let A and B be two central simple K-algebras. Then $A \otimes_K B$ is also a central simple K-algebra.*

Proof. By Theorem 1.6, $A \otimes_K B$ is simple. To prove that $Z(A \otimes B) \simeq K$ we take any non-zero element $0 \neq z = \sum_{i=1}^n a_i \otimes b_i \in Z(A \otimes B)$ with the b_i's linearly independent over K. For any $c \in A$ we have

$$0 = (c \otimes 1)z - z(c \otimes 1) = \sum_{i=1}^{n} (ca_i - a_i c) \otimes b_i.$$

Thus since the b_i's are linearly independent, $ca_i = a_i c$ for any $c \in A$, i.e. $a_i \in Z(A) = K$ for any i. Hence we can rewrite z as $z = 1 \otimes b$ onde $b = \sum_{i=1}^n a_i b_i \neq 0$. But $(1 \otimes d)z - z(1 \otimes d) = 1 \otimes (db - bd)$ for all $d \in B$ implies $db = bd$ for all d and hence $b \in Z(B) = K$, i.e. $z = \lambda(1 \otimes 1)$. Identifying K with $K(1 \otimes 1)$ we proved that $Z(A \otimes B) = K$. ∎

Theorem 1.16 *The Brauer group is an abelian group whose operation is the tensor product.*

Proof. We already saw that $A \otimes B$ is a central simple K-algebra whenever A and B are central simple. Obviously $A \otimes B \simeq B \otimes A$ and hence $[A \otimes B] = [B \otimes A]$. The neutral element of this operation is $[K]$. Let A be any finite dimensional central simple K-algebra and denote by A^{op} its opposite algebra, i.e. the K-algebra whose underlying additive abelian group is A, but whose multiplication is $a \cdot b := ba$ for all $a, b \in A$. A^{op} is again a central simple K-algebra with $\dim_K(A^{op}) = \dim_K(A) = n$. Hence by 1.15 $A^e := A \otimes A^{op}$ is central simple of dimension n^2. Since A is an A-bimodule, there exists a left A^e-module action on A given by $(x \otimes y)a = xay$ for all $x, y, a \in A$ which defines an algebra homomorphism $\varphi : A^e \to \mathrm{End}_K(A)$ since A^e is simple and $\dim_K(A^e) = n^2 = \mathrm{End}_K(A)$, φ is an isomorphism. On the other hand $\mathrm{End}_K(A) \simeq M_n(K)$. Thus

$$[A][A^{op}] = [A \otimes A^{op}] = [M_n(K)] = [K].$$

∎

1.3 Maximal subfields

Let $K \subseteq L$ be a field extension, then

$$\mathrm{Br}(K) \longrightarrow \mathrm{Br}(L)$$

$$[A] \longmapsto [A \otimes_K L]$$

is a group homomorphism and its kernel is denoted by $\mathrm{Br}(L/K)$ and called the **relative Brauer group**. Note that $[A] \in \mathrm{Br}(L/K)$ if and only if there are $n, m \geq 0$ such that $A \otimes_K M_n(L) \simeq M_m(L)$.

Let A be a simple K-algebra. A **maximal subfield** of A is a field $L \subseteq A$ which contains K such that $L = C(L) := \{a \in A : \forall x \in L : ax = xa\}$.

Theorem 1.17 *Let A be a central simple K-algebra of dimension n^2. Then for any maximal subfield L of A, we have $A \otimes_K L \simeq M_n(L)$.*

Proof. [4, Theorem 4.4.] ∎

The existence of maximal subfields in division algebras is given by the so-called **Jacobson-Noether** theorem:

Theorem 1.18 *Let D be a finite dimensional central divison algebra over K. Then there exists a maximal subfield L of D which is a separable extension of K.*

Proof. [5, 4.3.3] ∎

Recall that a field extension $K \subseteq L$ is called **normal** if every over K irreducible polynomial which has a root in L decomposes into linear factors in $L[X]$. A extension $K \subseteq L$ is called **Galois** if it is normal and separable. As a consequence we have the following important corollary which makes it easier to examine the Brauer group

Corollary 1.19 $\mathrm{Br}(K) = \bigcup\{\mathrm{Br}(L/K) \mid K \subseteq L \text{ is a finite Galois extension}\}$

Proof. Any $[A] \in \mathrm{Br}(K)$ can be represented by a finite dimensional central division algebra D over K, i.e. $[A] = [D]$.

By Theorem 1.18 there exists a separable extension F of K which is a maximal subfield of D. Then by 1.17 there exists $n \geq 1$ such that $D \otimes_K F \simeq M_n(F)$. Let $K \subseteq F \subseteq L$ be the normal closure. Then L is a finite Galois extension of K. Since

$$D \otimes_K L \simeq (D \otimes_K F) \otimes_F L \simeq M_n(F) \otimes_F L \simeq M_n(L),$$

we have $D \in \mathrm{Br}(L/K)$. ∎

1.4 Crossed Products

The last section allows us to reduce to finite dimensional central simple algebras which have maximal subfields which are finite Galois extensions.

First note the following situation: Let $K \subseteq L$ be a finite Galois extension with Galois group $G = Gal(L/K)$. Set $A = \mathrm{End}_K(L)$. Then $A \simeq M_n(K)$ for some $n = [L : K]$. Since each automorphism $g \in G$ fixes the elements of K, we might consider them as K-linear endomorphisms in A. It is well-known that they are L-linearly independent; here A is naturally a L-vector space by $(af)(x) := af(x)$ for all $a, x \in L$ and $f \in A$. Since $\dim_K(A) = n^2$ we have $\dim_L(A) = n$ and hence the elements of G form a basis. Thus any element of A can be written as $\sum_{g \in G} a_g g$.

Note that $a_g g$ represents the endomorphism that sends $x \in L$ to $a_g g(x)$. Hence the composition of endomorphisms yields

$$(a_g g)(b_h h)(x) = a_g g(b_h h(x)) = a_g g(b_h) gh(x) = [a_g g(b_h) gh](x)$$

Thus the multiplication in A is given by

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g h(b_h) gh.$$

What we actually have is a so-called **skew-group ring** of L and G, i.e. $A = L * G$. For any group action G on a ring R, i.e. a group homomorphism $G \to Aut(R)$ we might define the free R-module with basis the elements in G and the above multiplication. But also certain modification of this multiplication will yield an associative ring structure as we will now point out:

Take again our finite Galois extension $K \subseteq L$ with Galois group $G = Gal(L/K)$. Let $\gamma : G \times G \to L^* = L \setminus \{0\}$ be any map and $L *_\gamma G$ the vector space over L with dimension $n = [L : K]$. Choose a basis $\{v_g \mid g \in G\}$ of $L *_\gamma G$ and define a multiplication by

$$\left(\sum_{g\in G} a_g v_g\right)\left(\sum_{h\in G} b_h v_h\right) = \sum_{g,h\in G} a_g h(b_h)\gamma(g,h) v_{gh}.$$

If $\gamma(g, h) = 1$ for all g, h, we get the multiplication of $L * G$.

Lemma 1.20 *$L *_\gamma G$ is an associative algebra if and only if γ satisfies the* **cocycle condition**, *i.e. for all $g, h, k \in G$:*

$$\gamma(g,h)\gamma(gh,k) = \gamma(g,hk)g(\gamma(h,k))$$

In this case γ is called a **2-cocycle of G with values in L^***.

Definition 1.21 *$Z^2(G, L^*)$ denotes the set of 2-cocycles of G with values in L^*, i.e.*

$$Z^2(G,L^*) = \{\gamma : G \times G \to L^* \mid \forall g,h,k \in G : \gamma(g,h) = \gamma(g,hk)g(\gamma(h,k))\gamma(gh,k)^{-1}\}.$$

For each $\gamma \in Z^2(G, L^*)$ the algebra $L *_\gamma G$ is called a **crossed product.**

Theorem 1.22 *Let $K \subseteq L$ be any finite Galois extension with $G = Gal(L/K)$.*

1. *For any $\gamma \in Z^2(G, L^*)$ is the crossed product $L *_\gamma G$ a finite dimensional central simple K-algebra with maximal subfield L, i.e. $[L *_\gamma G] \in \mathrm{Br}(L/K)$.*
2. *For any $[A] \in \mathrm{Br}(L/K)$ there exists $\gamma \in Z^2(G, L^*)$ such that $[A] = [L *_\gamma G]$.*

PROOF. [4, 4.9,4.10] ∎

We need some group cohomology to make the correspondence between 2-cocylces and elements of the relative Brauer group precise

Note that $Z^2(G, L^*)$ becomes an abelian group with pointwise multiplication, i.e. if γ_1 and γ_2 are in $Z^2(G, L^*)$ then $\gamma_1\gamma_2(g, h) = \gamma_1(g, h)\gamma_2(g, h)$. The unit element is the 2-cocylce that maps everything to 1. Consider the following subgroup of $Z^2(G, L^*)$:

$$B^2(G,L^*) = \{\gamma \in Z^2(G,L^*) \mid \exists f : G \to L^*,\ \forall g,h \in G : \gamma(g,h) = g(f(h))f(gh)^{-1}f(h)\}$$

The quotient group $H^2(G, L^*) = Z^2(G, L^*)/B^2(G, L^*)$ is called the second cohomology group of G with coefficients in L^*.

Theorem 1.23 *For any finite Galois extension $K \subseteq L$ with Galois group $G = Gal(L/K)$ the map*

$$H^2(G, L^*) \longrightarrow \mathrm{Br}(L/K)$$
$$[\gamma] \mapsto [L *_\gamma G]$$

is an isomorphism of groups.

PROOF. [4, 4.13] ∎

Take $\gamma \in Z^2(G, L^*)$, then for all $g, h, k \in G$:

$$\gamma(g, h) = \gamma(g, hk)g(\gamma(h, k))\gamma(gh, k)^{-1}$$

Multiplying over all $k \in G$ and setting $f(x) = \prod_{k\in G} \gamma(x, k)$ we have

$$\begin{aligned} \gamma(g, h)^{|G|} &= \left(\prod_{k\in G} \gamma(g, hk)\right) g \left(\prod_{k\in G} \gamma(h, k))\right) \left(\prod_{k\in G} \gamma(gh, k)^{-1}\right). \\ &= f(g)g(f(h))f(gh)^{-1} \in B^2(G, L^*). \end{aligned}$$

Hence $H^2(G, L^*)$ is a torsion group and we conclude:

Corollary 1.24 *The Brauer group of a field is a torsion group.*

Chapter 2

Azumaya Algebras

The Brauer group of a commutative ring was defined by Auslander and Goldman in [2] by introducing the notion of an algebra A which is separable over a commutative ring R. At the same time G.Azumaya studied algebras which are separable over its center. Some time later Hirata and Sugano introduced non-commutative separable ring extension. This will be our starting point to discuss shortly the Brauer group of a commutative ring and basic properties of Azumaya algebras.

2.1 Separable extensions

Definition 2.1 *Let $R \subseteq S$ be a ring extension. Then S is* **separable** *over R if the map*

$$\mu : S \otimes_R S \to S$$

$$a \otimes b \mapsto ab$$

splits as S-bimodule map.

Here $S \otimes_R S$ is an S-bimodule by $s(a \otimes b)t = (sa) \otimes (bt)$ for all $s, t, a, b \in S$. The condition is equivalent to the existence of a **separability idempotent:**

$$e = \sum_{i=1}^{n} x_i \otimes y_i \in S \otimes S$$

such that $\mu(e) = 1$ and for all $s \in S : se = es$, i.e.

$$\sum_{i=1}^{n} sx_i \otimes y_i = \sum_{i=1}^{n} x_i \otimes y_i s.$$

Remark 2.2 *A typical example of separable extension is given by matrix rings. Let R be any (associative, unital) ring, $n \geq 1$ and $S = M_n(R)$ the ring of n by n matrizes over R. Identifying R with $R1_S$ we might think of S as a ring extension of R. Let E_{ij} denote the canonical basis elements of S. Recall that $E_{ij}E_{kl} = \delta_{j,k}E_{il}$. The element*

$$e = \sum_{i=1}^{n} E_{i1} \otimes E_{1i}$$

is a separability idempotent of S over R. First note that

$$\mu(e) = \sum_{i=1}^{n} E_{i1}E_{1i} = \sum_{i=1}^{n} E_{ii} = 1_S.$$

And for an arbitrary basis matrix E_{kl} we have

$$E_{kl}e = \sum_{i=1}^{n} E_{kl}E_{i1} \otimes E_{1i} = \sum_{i=1}^{n} \delta_{l,i}E_{k1} \otimes E_{1i} = E_{k1} \otimes E_{1l}$$

$$eE_{kl} = \sum_{i=1}^{n} E_{i1} \otimes E_{1i}E_{kl} = \sum_{i=1}^{n} E_{i1} \otimes \delta_{i,k}E_{1l} = E_{k1} \otimes E_{1l}.$$

Thus $se = es$ for any $s \in S$.

One of the most important properties of separable extensions $R \subseteq S$ is that homological properties of the category of R-modules transfers to the category of S-modules.

Theorem 2.3 *A separable extension $R \subseteq S$ is semisimple, i.e. every exact sequence in S-Mod that splits in R-Mod, also splits in S-Mod.*

PROOF. Let $e = \sum_{i=1}^{n} x_i \otimes y_i \in S \otimes S$ be a separable idempotent for S over R. For any left S-modules M, N and left R-linear map $f : M \to N$ we can define a map $\overline{f} : M \to N$ by

$$(m)\overline{f} = \sum_{i=1}^{n} x_i(y_i m)f$$

for all $m \in M$, which is left S-linear, since $se = es$ for all $s \in S$implies

$$(sm)\overline{f} = \sum_{i=1}^{n} x_i(y_i sm)f = \sum_{i=1}^{n} sx_i(y_i m)f = s(m)\overline{f}.$$

Let $f : M \to N$ be an (S-linear) epimorphism of S-modules which splits as left R-modules, then there exists $g : N \to M$ such that $((n)g)f = n$ for all $n \in N$. Hence

$$(n)\overline{g}f = \left(\sum_{i=1}^{n} x_i(y_i n)g\right) f = \sum_{i=1}^{n} x_i((y_i n)g)f = \sum_{i=1}^{n} x_i(y_i n) = \left(\sum_{i=1}^{n} x_i y_i\right) n = n$$

for all $n \in N$. Hence $\overline{g}$ splits f in S-Mod. ∎

In particular we have that every S-module which is projective as R-module is projective as S-module.

2.2 Algebras over commutative rings

Let R be a commutative ring and A an R-algebra, i.e. A is an R-module, there exists a map $R \to R1_A \subseteq Z(A)$ and the multiplication of A is R-bilinear. Define $A^e := A \otimes_R A^{op}$ which is an associative algebra. Denote by

$$L_a : [x \to ax] \quad \text{and} \quad R_b : [x \to xb]$$

the left resp. right multiplication maps of elements $a, b \in A$ which are R-linear, i.e. $L_a, R_b \in \mathrm{End}_R(A)$. Then A becomes a left A^e-module by $(a \otimes b)x = L_a(R_b(x)) = axb$ or equivalently by the ring homomorphism

$$\psi : A^e = A \otimes_R A^{op} \longrightarrow \mathrm{End}_R(A) \quad a \otimes b \mapsto L_a \circ R_b$$

The center of A is isomorphic to the endomorphism ring of A as A^e-module given by the map

$$\phi : \mathrm{End}_{A^e}(A) \longrightarrow Z(A) \quad f \mapsto f(1).$$

Well, we check easily that $f(1)$ is central, since

$$af(1) = f(a1)f(a) = f(1a) = f(1)a$$

for all $a \in A$. And for two endomorphisms f, g we have

$$\phi(f \circ g) = f(g(1)) = f(1g(1)) = f(1)g(1) = \phi(f)\phi(g).$$

The inverse of ϕ is given by $x \mapsto L_x : [a \mapsto xa]$ for all $x \in Z(A)$.

Moreover for any A-bimodule, i.e. left A^e-module, M the center of M is defined as

$$Z(M) = \{m \in M \mid \forall a \in A : am = ma\},$$

which is a $Z(A)$-submodule of M. Also here we can establish a connection between the center of a bimodule and certain homomorphisms, namely

$$\phi_M : \mathrm{Hom}_{A^e}(A, M) \longrightarrow Z(M)$$

$$f \mapsto f(1)$$

is an isomorphism of $Z(A)$-modules whose inverse is given by $x \mapsto L_x : [a \mapsto xa]$. In particular we can show that

$$\mathrm{Hom}_{A^e}(A, -) : A^e - \mathrm{Mod} \longrightarrow Z(A) - \mathrm{Mod}$$

is a functor from the category of A-bimodules to the category of modules over the center of A.

Lemma 2.4 *Let A be an R-algebra. Then $R \cdot 1_A \subseteq A$ is separable if and only if A is a projective A^e-module.*

Proof. Set $\overline{R} = R \cdot 1_A$ and assume that A is separable over $\overline{R}$. Then there exists a separability idempotent $e \in A \otimes_{\overline{R}} A$. Note that the A-bimodule structure on A is defined by the left A^e-module structure on A. Hence the epimorphism $\mu : A^e \to A$ splits by $\beta : A \to A^e$ with $\beta(a) = ae$ as A^e-module. On the other hand if μ splits by an A-bimodule map $\beta : A \to A^e$, then choose $e = \beta(1_A)$ for the desired separability idempotent. ∎

We might always assume A to be a faithful R-module by going to the factor ring

$$\overline{R} = R/\mathrm{Ann}_R(A) \simeq R \cdot 1_A.$$

Then $A^e = A \otimes_R A^{op} = A \otimes_{\overline{R}} A^{op}$. Note that A being a projective A^e-module is equivalent to say that the functor $\mathrm{Hom}_{A^e}(A, -)$ is exact.

Definition 2.5 *We also say for short that A is separable over R if A is separable over $R \cdot 1_A$ even if A is not faithful.*

If A is a separable R-algebra and projective as R-module, then it has to be also finitely generated as R-module as the following theorem proves:

Theorem 2.6 *Let A be a separable R-algebra. If A_R is projective, then A_R is finitely generated.*

Proof. We might suppose that A is a faithful R-module and that R embedds into A. Since A_R is projective also A^{op} is projective as R-module and has a dual basis $(b_\lambda, p_\lambda)_{\lambda \in \Lambda}$ for some elements $b_\lambda \in A^{op}$ and $p_\lambda \mathrm{Hom}_R(A^{op}, R)$. There are homomorphisms

$$\begin{array}{ccccc} A^{op} & \xrightarrow{f} & R^{(\Lambda)} & \xrightarrow{g} & A^{op} \\ y & \xrightarrow{f} & ((y)p_\lambda)_\Lambda & \xrightarrow{g} & \sum_{\lambda \in \Lambda} (y)p_\lambda b_\lambda \end{array}$$

satisfying $((a)f)g = a$ for all $a \in A$. Applying $A \otimes_R -$ we get the maps

$$\begin{array}{ccccc} A \otimes_R A^{op} & \xrightarrow{id\otimes f} & A \otimes_R R^{(\Lambda)} & \xrightarrow{id\otimes g} & A \otimes_R A^{op} \\ x \otimes y & \longrightarrow & (x \otimes (y)p_\lambda)_\Lambda & \longrightarrow & \sum_{\lambda\in\Lambda} x \otimes (y)p_\lambda b_\lambda \end{array}$$

and $(x \otimes y)(id \otimes f)(id \otimes g)$. Let $e = \sum_{i=1}^n x_i \otimes y_i$ be a separable idempotent for A over R. For any $a \in A$ we have

$$ae = (a \otimes 1)e = [(a \otimes 1)(id \otimes f)(id \otimes g)]\, e = \sum_{i=1}^n ax_i \otimes \sum_{\lambda\in\Lambda} (y_i)p_\lambda b_\lambda$$

$$ea = e(1 \otimes a) = \left(\sum_{i=1}^n x_i \otimes y_i a\right)(id \otimes f)(id \otimes g) = \sum_{i=1}^n x_i \otimes \sum_{\lambda\in\Lambda} (y_i a)p_\lambda b_\lambda$$

Set $\Lambda' = \{\lambda \in \Lambda \mid \exists i : (y_i)p_\lambda \neq 0\}$. Then Λ' is finite. Thus

$$\sum_{\lambda\in\Lambda'} \left(\sum_{i=1}^n ax_i(y_i)p_\lambda\right) \otimes b_\lambda = ae = ea = \sum_{\lambda\in\Lambda} \left(\sum_{i=1}^n x_i(y_i a)p_\lambda\right) \otimes b_\lambda$$

implies that also

$$ea = \sum_{\lambda\in\Lambda'} \left(\sum_{i=1}^n x_i(y_i a)p_\lambda\right) \otimes b_\lambda.$$

Applying the multiplication μ, we get

$$a = \mu(ea) = \sum_{\lambda\in\Lambda'} \sum_{i=1}^n x_i(y_i a)p_\lambda b_\lambda = \sum_{i=1}^n \sum_{\lambda\in\Lambda'} (y_i a)p_\lambda x_i x_i b_\lambda$$

which shows that $\{x_i b_\lambda\}_{1\leq i\leq n, \lambda\in\Lambda'}$ is a finite generating set of A as R-module. ∎

2.3 Central separable algebras

Definition 2.7 *A central R-algebra A is called* **Azumaya** *if it is central, i.e. $R = Z(A)$ and separable over R.*

We first show that for finite dimensional K-algebras this notion coincides with the notion of a finite dimensional central simple K-algebra

Theorem 2.8 *Let A be a K-algebra over a field K. Then A is an Azumaya algebra if and only if it is a finite dimensional central simple K-algebra.*

Proof. Let $Z(A) = K$ and A be separable over K, then Theorem 2.6 shows that A is finite dimensional. Moreover Theorem 2.3 shows that every exact sequence in A-Mod splits, i.e. A is semisimple artinian. Thus by the Wedderburn-Artin Theorem A is a finite product of matrix rings of division rings. Since the center of A is K, i.e. indecomposable, $A \simeq M_n(D)$ for a finite dimensional divison algebra D over K. Thus A is a finite dimensional central divison algebra over K.

On the contrary, suppose that $A = M_n(D)$ with $Z(A) = Z(D) = K$. From the fact that the inverse of $[A]$ in the Brauer group is $[A^{op}]$ (see Theorem 1.16) we have that $A \otimes A^{op} \simeq M_m(K)$ for some $m \geq 1$. Hence $A \otimes A^{op}$ is a semisimple algebra, and hence any A-bimodule is projective. So is A itself, which says that A is separable over $K = Z(A)$ by Lemma 2.4. ∎

In the following Lemma we gather more information on separable algebras over commutative rings.

Lemma 2.9 *Let R be a commutative ring and A an R-algebra which is separable over R.*

1. *Suppose that S is a commutative R-algebra such that A is an S-algebra extending its R-algebra structure, then A is also separable over S.*
2. *If I is an ideal of R, then A/IA is separable over R/I.*
3. *If I is an ideal of $Z(A)$, then $I = Z(A) \cap IA$ and $Z(A/IA) = Z(A)/I$.*
4. *For any maximal ideal I of A, $I = mA$ for some maximal ideal m of $Z(A)$.*

PROOF. (1) Note that there exists an exact sequence of R-modules:

$$0 \longrightarrow \longrightarrow K \longrightarrow A \otimes_R A \xrightarrow{p} A \otimes_S A \longrightarrow 0$$

where K is generated by all elements of the form $as \otimes b - a \otimes sb$ for $a, b \in A$ and $s \in S$. Let $e \in A \otimes_R A$ be a separable idempotent for A over R, then $p(e) \in A \otimes_S A$ is a separable idempotent of A over S.

(2) Note that

$$A/IA \otimes_{R/I} A/IA \simeq (A \otimes_R R/I) \otimes_{R/I} (R/I \otimes_R A) = A \otimes_R (R/I \otimes_{R/I} R/I) \otimes_R A \simeq A \otimes_R A \otimes_R R/I.$$

Thus the separability idempotent of A over R can be lifted to one of A/IA over R/I.

(3) Let I be an ideal in $Z(A)$. Any element $x \in Z(A) \cap (IA)$ can be seen as a A^e-linear map $L_x : [a \mapsto xa]$ of A. Writing $x = \sum_{i=1}^n y_i a_i$ with $y_i \in I$ and $a_i \in A$ we consider the projection $p : A^n \to \sum_{i=1}^n y_i A =: J \subset IA$. Since A is projective in A^e-Mod, the diagram

$$\begin{array}{ccccc} & & A & & \\ & & \downarrow{\scriptstyle L_x} & & \\ A^n & \xrightarrow{p} & J & \longrightarrow & 0 \end{array}$$

can be extended by an A^e-linear map $g : A \to A^n$ such that

$$x = L_x(1) = p(g(1)) = p(z_1, \ldots, z_n) = \sum_{i=1}^n y_i z_i$$

for some $z_i \in Z(A)$ obtained by identifying $g(1) \in Z(A^n) = Z(A)^n$. Thus $x \in I$.

Apply the exact functor $\mathrm{Hom}_{A^e}(A, -)$ to the exact sequence

$$0 \longrightarrow IA \longrightarrow A \longrightarrow A/IA \longrightarrow 0.$$

Then we get and exact sequence of $\mathrm{End}_{A^e}(A)$-modules

$$0 \longrightarrow \mathrm{Hom}_{A^e}(A, IA) \longrightarrow \mathrm{End}_{A^e}(A) \longrightarrow \mathrm{Hom}_{A^e}(A, A/IA) \longrightarrow 0.$$

Identifying $\mathrm{Hom}_{A^e}(A, M)$ for an A-bimodule M with its center $Z(M)$ we have an exact sequence

$$0 \longrightarrow Z(IA) = Z(A) \cap (IA) \longrightarrow Z(A) \longrightarrow Z(A/IA) \longrightarrow 0.$$

Since we showed that $Z(A) \cap (IA) = I$, we have $Z(A/IA) = Z(A)/I$.

(4) Let I be a maximal ideal of A and consider the ideal $m = I \cap Z(A)$ of $Z(A)$. Since $Z(A)$ is a commutative R-algebras, we have by (1) that A is also a separable $Z(A)$-algebra. By (2) A/mA is separable over $Z(A)/m$ which is a field. Since $Z(A/mA) = Z(A)/m$ by (3), A/mA is an Azumaya algebra over $Z(A)/m$ and by Theorem 2.8 is a central simple algebra, i.e. mA is a maximal ideal forcing $mA = I$. ∎

We will now state the main characterisation of Azumaya algebras, but for its proof we need some results in module theory that we will subsequently present. Recall that a functor $F : \mathbb{C} \to \mathbb{D}$ between two categories is an equivalence if there exists a functor $G : \mathbb{D} \to \mathbb{C}$ and functorial isomorphisms $\eta_X : G(F(X)) \to X$ and $\mu_Y : Y \to F(G(Y))$ for all $X \in \mathbb{C}$ and $Y \in \mathbb{D}$.

Theorem 2.10 *Let A be a central K-algebra with K a commutative ring. The following statements hold:*

(a) A is an Azumaya algebra;

(b) A is generator in A^e-Mod;

(c) The functor $Z(-) : A^e - \mathrm{Mod} \to K - \mathrm{Mod}$ defines an equivalence of categories with inverse $A \otimes_K - : K - \mathrm{Mod} \to A^e - \mathrm{Mod}$

(d) A is a finitely generated projective K-module, such that $\psi : A^e \to \mathrm{End}_K(A)$ is an isomorphism.

PROOF. $(a) + (b) \Rightarrow (c)$ follows from the Morita theorems (see [8] for example) which says that $\mathrm{Hom}_R(M, -)$ is an equivalence of categories between R-Mod and Mod-$\mathrm{End}_R(S)$ with inverse $M \otimes_S -$ for any finitely generated projective generator M in R-Mod. Since $Z(-) \simeq \mathrm{Hom}_{A^e}(A, -)$ it follows that $Z(-)$ is an equivalence whose inverse is $A \otimes_K -$.

$(c) \Rightarrow (a) + (b)$ If $Z(-) \simeq \mathrm{Hom}_{A^e}(A, -)$ is an equivalence then it is exact, i.e. A is projective as A^e-module which means that A is Azumaya by Lemma 2.4. Since for any A-bimodule X we have

$$X \simeq A \otimes_K Z(X) \simeq AZ(K) = A\mathrm{Hom}_{A^e}(X, =) : Tr(A, X)$$

where $Tr(M, N)$ is called the trace of M in N, we have that A is a generator in A^e-Mod.

(a) $\Rightarrow$ (b): Suppose A is Azumaya, i.e. there exists a separable idempotent $e = \sum_{i=1}^n x_i \otimes y_i \in A \otimes A$. Then

$$f = \sum_{i,j=1}^{n} (x_i \otimes y_j) \otimes (y_i \otimes x_j)$$

is a separable idempotent for A^e over A, i.e. the extension $A \subseteq A^e$ is separable. Let $T = \mathrm{Tr}(A, A^e)$ be the trace of A in A^e. It is enough to show that $T = A^e$ since in this case A generates A^e. Suppose that $T \neq A^e$, then there exists a maximal ideal M of A^e such that $T \subseteq M$. By Lemma 2.9 there exists a maximal ideal m of $Z(A^e)$ with $mA^e = M$. Note that

$$Z(A^e) = Z(A) \otimes_K Z(A) = K(1 \otimes 1) \simeq K.$$

Hence mA is a two-sided ideal of A, but since

$$A = TA = MA = mA^eA = mA$$

it is improper, what is impossible, because $A = mA$ implies that $m = Z(A) \cap (mA) = Z(A)$ by Lemma 2.9. Thus the trace ideal T has to equal A^e what shows that A is a generator in A^e-Mod.

(b) $\Leftrightarrow$ (d): This implication will follow from a general module theoretical result (see below). In our setting $R = A^e$, $M = A$ and $S = \mathrm{End}_{A^e}(A) \simeq Z(A) = K$ as A is supposed to be a central K-algebra. Then Theorem 2.11 says that A is a generator in A^e-Mod if and only if A is finitely generated projective as K-module and $A^e \simeq \mathrm{End}_K(A)$.

■

Let R be a associative ring with unit (possibly non-commutative) and let M be a left R-module with endomorphism ring S. Then M is a right S-module and its endomorphism ring $T = \mathrm{End}_S(M_S)$ is called the biendomorphism ring of M. There exists a natural ring homomorphism $\psi : R \to T$ sending $r \in R$ to $L_r : [m \mapsto rm]$ which is right S-linear. Note that $\ker(\psi) = \mathrm{Ann}_R(M)$.

Theorem 2.11 (Characterisation of generators) *A left R-module M with endomorphism ring S and biendomorphism ring T is a generator in R-Mod if and only if M_S is finitely generated projective and $\psi : R \simeq T$ is an isomorphism.*

PROOF. Suppose first that M_S is finitely generated and projective and that $R \simeq T = \mathrm{End}_S(M_S)$. Then there exists $n \in \mathbb{N}$ and an exact sequence of right S-modules

$$0 \longrightarrow D_S \longrightarrow S^n \longrightarrow M_S \longrightarrow 0$$

which splits as M_S is projective. Hence applying the functor $\mathrm{Hom}_S(-, M_S)$ we also get a splitting exact sequence in $R \simeq \mathrm{End}_S(M)$-Mod:

$$0 \longrightarrow \mathrm{Hom}_S(D_S, M_S) \longrightarrow \mathrm{Hom}_S(S^n, M_S) = M^n \longrightarrow \mathrm{Hom}_S(M_S, M_S) \simeq R \longrightarrow 0$$

Hence M generates R as left R-module.

For the converse assume that M generates R as left R-module. Then there exists a splitting short exact sequence

$$0 \longrightarrow D \longrightarrow M^n \longrightarrow R \longrightarrow 0$$

Applying the functor $\mathrm{Hom}_R(-, M)$ we obtain a splitting short exact sequence in Mod-S:

$$0 \longrightarrow \mathrm{Hom}_R(D, M) \longrightarrow \mathrm{Hom}_R(M, M^n) \simeq S^n \longrightarrow \mathrm{Hom}_R(R, M) = M_S \longrightarrow 0$$

which shows that M_S is finitely generated projective. To show that $R \simeq T$ we need, what's sometimes is called the "Density theorem": Since M is finitely generated as right S-module, there are elements $x_1, \ldots, x_n$ such that $M = \sum_{i=1}^n x_i S$. Consider the cyclic submodule $N := R(x_1, \ldots, x_n) \subseteq M^n$. Since M is a generator, there exists a number k and an epimorphism $f : M^k \to N \subseteq M^n$. We might consider f as an endomorphism of the module $M^{max(k,n)}$ and hence can assume, without loss of generality, that $n = k$ and $f : M^n \to M^n$. Note that any biendomorphism $\beta : M \to M$ can be seen as a biendomorphism of M^n by setting

$$\beta(m_1, \ldots, m_n) = (\beta(m_1), \ldots, \beta(m_n))$$

for all $(m_1, \ldots, m_n) \in M^n$. A technical argument shows that β is $\mathrm{End}_R(M^n)$-linear. Thus

$$(\beta(x_1), \ldots, \beta(x_n)) \in \beta(N) = \beta[(M^n)f] = [\beta(M^n)]f \subseteq N = R(x_1, \ldots, x_n)$$

which implies that there exists $r \in R$ with $rx_i = \beta(x_i)$. Hence the biendomorphism is given by right multiplication of r, i.e. for any $m = \sum_{i=1}^n (x_i) f_i \in M$ for $f_i \in S$ we have

$$\beta(m) = \sum_{i=1}^n \beta((x_i)f_i) = \sum_{i=1}^n (\beta(x_i))f_i = \sum_{i=1}^n (rx_i)f_i = rm.$$

This shows that $\psi : R \to \mathrm{End}_S(M_S)$ is surjective. Since M is a generator, it must be faithful, i.e. ψ is an isomorphism. ∎

2.4 The Brauer group of a commutative ring

Separable R-algebras A which are finitely generated over R can be characterised by a local-global argument.

Theorem 2.12 *Let A be an R-algebra which is finitely generated as R-module. Then A is separable over R if and only if A_m is separable over R_m for every maximal ideal m of R,*

PROOF. [9, 28.9] ∎

This local-global argument allows a quick prove of the following:

Corollary 2.13 *If P is a finitely generated, projective R-module, then $\mathrm{End}_R(P)$ is a separable R-algebra.*

PROOF. Since for any maximal ideal m of R we have

$$\mathrm{End}_R(P)_m \simeq \mathrm{End}_R(P) \otimes_R R/m \simeq \mathrm{End}_{R/m}(P/mP)$$

given by $f \otimes \overline{a} \mapsto [p \mapsto f(p)\overline{a}]$. On the left we have the endomorphism ring of a finite dimensional vector space over R/m, i.e. $\mathrm{End}_{R/m}(P/mP) \simeq M_k(R/m)$ is a finite dimensional central simple algebra. Hence by Theorem 2.12, $\mathrm{End}_R(P)$ is separable over R. ∎

In particular one can show that if P is a progenerator, i.e. a finitely generated projective generator in R-Mod, then $\mathrm{End}_R(P)$ is an Azumaya algebra over R.

Definition 2.14 *Let A and B be two Azumaya algebras over R. We write $A \sim B$ if there exist progenerators ${}_RP$ and ${}_RQ$ such that $A \otimes_R \mathrm{End}_R(P) \simeq B \otimes_R \mathrm{End}_R(Q)$,*

Note that if $A \sim B$ e $B \sim C$ for three Azumaya algebras A, B, C over R, then there R-progenerators P, Q, P', Q' such that $A \otimes \mathrm{End}_R(P) \simeq B \otimes \mathrm{End}_R(Q)$ and $B \otimes \mathrm{End}_R(P') \simeq C \otimes \mathrm{End}_R(Q')$. To conclude that $A \sim C$ it is now enough to verify that $\mathrm{End}_R(P \otimes P') \simeq \mathrm{End}_R(P) \otimes \mathrm{End}_R(P')$ for finitely generated projective R-modules, since then

$$\begin{aligned} A \otimes \mathrm{End}_R(P \otimes P') &\simeq A \otimes \mathrm{End}_R(P) \otimes \mathrm{End}_R(P') \\ &\simeq B \otimes \mathrm{End}_R(Q) \otimes \mathrm{End}_R(P') \\ &\simeq B \otimes \mathrm{End}_R(P') \otimes \mathrm{End}_R(Q) \\ &\simeq C \otimes \mathrm{End}_R(Q') \otimes \mathrm{End}_R(Q) \\ &\simeq C \otimes \mathrm{End}_R(Q' \otimes Q) \end{aligned}$$

Thus $\sim$ is an equivalence relation and we can define

Definition 2.15 *The* **Brauer group of a commutative ring** *R is the abelian group $\mathrm{Br}(R) = \{[A]_\sim \mid A$ is an Azumaya algebra over $R\}$ whose product is again the tensor product.*

Chapter 3

Group rings and Skew group rings

3.1 Group ring

Let G be group and R any ring (possibly non-commutative, but associative with unit).

Definition 3.1 *The* **group ring** *of G over R is the free R-module $R[G]$ with basis $\{\overline{g} \mid g \in G\}$ and multiplication*

$$(a\overline{g})(b\overline{h}) = ab\overline{gh}$$

for all $a, b \in R, g, h \in G$.

The map

$$\alpha : R[G] \to R \quad \sum a_g \overline{g} \mapsto \sum a_g$$

is a surjective ring homomorphism as one easily see by the definition of the multiplication of $R[G]$. The ideal $A = \mathrm{Ker}(\alpha)$ is called the augmentation ideal

Moreover R becomes a left $R[G]$-module induced by α whose $R[G]$-action is defined as $a\overline{g}\cdot x = ax$ for all $a, x \in R$ and $g \in G$.

Lemma 3.2 *Let $\mathcal{G}$ be a set of group generators of G, then $A = \mathrm{Ker}(\alpha)$ is generated as a left ideal of $R[G]$ by the elements $1 - \overline{g}$ for $g \in \mathcal{G}$.*

Proof. For any $\gamma = \sum a_g \overline{g} \in \mathrm{Ker}(\alpha)$, then $\sum a_g = 0$. Hence $\gamma = \sum -a_g(1 - \overline{g})$ and the ideal A is generated by $1 - \overline{g}$ for any $g \in G$. Suppose that $\mathcal{G}$ is a set of group generators of G. Then any $x \in G$ is a finite product of elements of $g \in \mathcal{G}$. Write x as $\sigma(1)\sigma(2)\cdots\sigma(k)$ for some function $\sigma : \{1, \ldots, k\} \to \mathcal{G}$. Then

$$\begin{aligned} 1 - \overline{x} &= 1 - \overline{\sigma(1)\sigma(2)\cdots\sigma(k)} \\ &= 1 - \overline{\sigma(1)} + \sum_{j=1}^{k-1} \overline{\sigma(1)\cdots\sigma(j+1)} - \overline{\sigma(1)\cdots\sigma(j)} \\ &= 1 - \overline{\sigma(1)} + \sum_{j=1}^{k-1} \overline{\sigma(1)\cdots\sigma(j)}(\overline{\sigma(j+1)} - 1) \end{aligned}$$

■

We denote the support of an element $\gamma = \sum_{g \in G} a_g \overline{g}$ of $R[G]$ by

$$supp(\gamma) = \{g \in G \mid a_g \neq 0\} \subseteq G.$$

By definition of $R[G]$, $supp(\gamma)$ is always a finite set (or empty for $\gamma = 0$).

Lemma 3.3 *If there exists* $0 \neq f \in \mathrm{Hom}_{R[G]}(R, R[G]) \neq 0$*, then* G *is finite and* $f(1) = rt$ *for some* $r \in R$ *where* $t = \sum_{g\in G} \overline{g}$*.*

PROOF. Let $f : R \to R[G]$ be a non-zero $R[G]$-linear map, then $f(a) = af(1)$ for all $a \in A$. Let $f(1) = \sum_{h\in H} a_h\overline{h}$ and $0 \neq a_h \in A$ for all $h \in H$ where $H = supp(f(1))$. For any $g \in G$ we have

$$\sum_{h\in H} a_h\overline{h} = f(1) = f(g \cdot 1) = \overline{g}f(1) = \sum_{h\in H} a_h\overline{gh} = \sum_{k\in gH} a_{g^{-1}k}\overline{k}, \tag{3.1}$$

i.e. $gH = H$ for any $g \in G$. Thus $G = H$ and hence G is finite. Furthermore by (3.1) $a_{g^{-1}k} = a_k$ for any $g \in G$, i.e. $a_g = a_e =: r$ for any $g \in G$. Thus $f(1) = r\sum_{g\in G} \overline{g} = rt$. ∎

Lemma 3.3 is a key observation (partly due to Angel del Rio), which implies that the projectivity of R over $R[G]$ makes G finite.

Corollary 3.4 *The following statements are euivalent:*

(a) $R \subseteq R[G]$ *is a separable extension;*

(b) R *is a projective* $R[G]$*-module*

(c) G *is finite and* $|G|1_R$ *is invertible in* R*.*

PROOF. $(a) \Rightarrow (b)$ is clear since separable extensions are semisimple by Theorem 2.3. Since α splits as R-linear map by $\beta(1) = 1\overline{e}$, it also splits as $R[G]$-linear map, which implies R being a projective $R[G]$-module.

$(b) \Rightarrow (c)$ If R is projective as $R[G]$-module, then the epimorphism α splits by some $\beta : R \to R[G]$. By Lemma 3.3, G is finite. Moreover $\beta(1) = rt$ where $t = \sum_{g\in G} \overline{g}$. Since

$$1 = \alpha(\beta(1)) = \sum_{g\in G} r = |G|r,$$

we see that $|G| = |G|1$ is invertible in R.

$(c) \Rightarrow (a)$ If G is finite and $|G|$ is invertible in R, then

$$e = \frac{1}{|G|}\sum_{g\in G} \overline{g}\otimes_R\overline{g^{-1}}$$

is a separable idempotent for $R[G]$ over R. Firstly l because

$$\mu(e) = \frac{1}{|G|}\sum_{g\in G} \overline{g}\overline{g^{-1}} = \frac{1}{|G|}|G|\overline{e} = 1_{R[G]}.$$

And secondly because for any $h \in H$:

$$he = \frac{1}{|G|}\sum_{g\in G} \overline{hg}\otimes_R\overline{g^{-1}} = \frac{1}{|G|}\sum_{k\in h^{-1}G} \overline{hk}\otimes_R\overline{k^{-1}} = \frac{1}{|G|}\sum_{g\in G} \overline{g}\otimes_R\overline{g^{-1}h} = eh.$$

∎

Corollary 3.4 has two applications:

Theorem 3.5 $R[G]$ *is semisimple artinian if and only if* R *is semisimple artinian and* G *has finite order which is invertible in* R*.*

PROOF. If $R[G]$ is semisimple artinian, then any $R[G]$-module is projective, hence so is also R. Thus $R \subseteq R[G]$ is separable and G is finite with $|G|$ invertible in R. Since the lattice of left ideals of R equals the lattice of left $R[G]$-submodules of R and R is a semisimple $R[G]$-module, R is also semisimple as R-module.

The converse follows from Theorem 2.3, since G being finite and $|G|$ being invertible implies $R \subseteq R[G]$ being separable by Corollary 3.4. Hence by Theorem 2.3 any $R[G]$-module is projective since it is projective as R-module. ∎

This yields the famous Maschke Theorem for group rings over fields.

Corollary 3.6 *Let K be a field and G a group. Then $K[G]$ is semisimple artinian if and only if G is finte and $char(K) \nmid |G|$.*

John von Neumann introduced a certain class of rings which somewhat behave as semisimple artinian ring, but not necessarilly fullfilling a finitness condition (like having finite length or being noetherian or having finite Goldie dimension):

A ring R is called von Neumann regular if for any $a \in R$ there exist $b \in R$ such that $a = aba$. Many authors have contributed to the theory of von Neumann regular rings. Here we will give a typical characterisation of those rings:

Theorem 3.7 *The following statements are equivalent for a ring R:*

1. *R is regular;*
2. *every principal (or finitely generated) left (or right) ideal of R is generated by an idempotent (J.v.Neumann, 1936)*
3. *every finitely generated submodule of a projective left (or right) R-module is a direct summand (I.Kaplansky,1958)*
4. *The weak global dimension of R is zero (M.Auslander, 1957)*
5. *Every left (or right) R-module is flat (M.Auslander, 1957)*
6. *Every short exact sequence in R-Mod is pure.*
7. *Every finitetly presented module is projective.*
8. *R/I is a flat left R-module for every left ideal I of R (M.Auslander, 1957)*
9. *For every left ideal L and right ideal K of R: $K \cap L = KL$ (M.Auslander, 1957)*

As in the semisimple artinian case we have that separable extensions of regular rings are regular.

Proposition 3.8 *Let $R \subseteq S$ be a separable extension. If R is regular, then also S.*

PROOF. Let M be any left S-module and suppose it is flat as R-module. Hence ${}_RM \simeq \lim P_\lambda$ for some finitely generated projective left R-modules P_λ. Thus

$$S \otimes_R M \simeq S \otimes_R \lim P_\lambda \simeq \lim(S \otimes_T P_\lambda).$$

shows that $S \otimes_R M$ is flat as left S-module as $S \otimes_R P_\lambda$ is a finitely generated projective left S-module. Consider the S-linear map: $\varphi : S \otimes_R M \longrightarrow M\ s \otimes m \mapsto sm$. φ splits as R-module map with $\psi : M \longrightarrow S \otimes_R M$ and $\psi(m) = 1 \otimes m$. As S is a semisimple extension of R, φ also splits as left S-module map and ${}_SM$ is flat. Hence if R is von Neumann regular, every left R-module is flat and thus every left S-module as well, as seen. ∎

Before we state the characterisation of von Neumann regular group rings given by Auslander and Villamayor, we introduce a usefull concept which allows to extend Proposition 3.8 slightly: Following A.Magid we call an extension $R \subseteq S$ **locally separable** if any element of S is contained in a subring $R \subseteq T \subseteq S$ such that $R \subseteq T$ is separable.

This condition is sufficient for a ring extension $R \subseteq S$ to encusre that S is regular if R is.

Lemma 3.9 *Let $R \subseteq S$ be loally separable. If R is regular, then also S is regular.*

PROOF. Let $a \in S$. Then by hypothesis, there exists a separable extension $R \subseteq T \subseteq S$ containing a. Since R is regular, by Proposition 3.8, T is regular. Hence there exist $b \in T \subseteq S$ such that $a = aba$, i.e. S is regular. ∎

A sufficient condition for $R \subseteq R[G]$ to be locally separable is given by the following

Lemma 3.10 *Suppose that*

- *G is locally finite, i.e. any finitely generated subgroup is finite.*
- *$|H|$ is invertible in R for any finite subgroup H of G.*

Then $R \subseteq R[G]$ is locally separable.

PROOF. Take any $\gamma \in \sum_{g\in G} a_g\overline{g} \in R[G]$ and let H be the subgroup of G generated by $supp(\gamma)$. Then $\gamma \in R[H]$. By hypothesis H is a finite subgroup whose order is invertible in R. By Corollary 3.4 $T = R[H]$ is separable. Hence $R \subseteq R[G]$ is locally separable. ∎

Finally we can characterize regular group rings.

Theorem 3.11 (Auslander-Vilamayor) *The following statements are equivalent for a ring R and a group G.*

(a) $R[G]$ is regular

(b) R is regular and G is locally finite and the order of any finite subgroup of G is invertible in R.

(c) R is regular and $R \subseteq R[G]$ is locally separable.

PROOF. $(a) \Rightarrow (b)$ Let $R[G]$ be regular and H any subgroup of G. Take $\gamma = \sum_{h\in H} a_h\overline{h} \in R[H]$. Then there exist $\gamma' = \sum_{g\in G} b_g\overline{g}$ such that $\gamma = \gamma\gamma'\gamma$, i.e.

$$\sum_{h\in H} a_h\overline{h} = \left(\sum_{h\in H} a_h\overline{h}\right)\left(\sum_{g\in G} b_g\overline{g}\right)\left(\sum_{k\in H} a_k\overline{h}\right) = \left(\sum_{h,k\in H, g\in G} a_h b_g a_k\overline{hgk}\right)$$

Note that $hkg \in H$ for $h, k \in H$ if and only if $g \in H$. Thus (by comparing coefficients) we have that

$$\sum_{h,k\in H, g\notin H} a_h b_g a_k\overline{hgk} = 0.$$

Set $\gamma'' = \sum_{g\in H} b_g\overline{g} \in R[H]$ we have $\gamma = \gamma\gamma''\gamma$, i.e. $R[H]$ is regular. In particular for $H = \{e\}$, R is regular.

To see that G is locally finite, take any finitely generated subgroup H of G and suppose that H is generated (as a group) by $\mathcal{G} = \{g_1, \ldots, g_n\}$. By Lemma 3.2, the augementation ideal $K = \mathrm{Ker}(\alpha : R[H] \to R)$ is generated by all elements $1 - \overline{g_i}$ for $1 \leq i \leq n$. In particular K is finitely generated, i.e. R is finitely presented as $R[H]$-module. and hence projective, since $R[H]$ is regular. By 3.4 H is finite and its order invertible in R.

$(b) \Rightarrow (c)$ follows from Lemma 3.10 and $(c) \Rightarrow (a)$ from 3.9. ∎

DeMeyer and Janusz proved when a group ring $R[G]$ is Azumaya:

Theorem 3.12 *Let G be a group with center $Z(G)$ and commutator G'. Then $R[G]$ is an Azumaya algebra if and only if*

1. *R is an Azumaya algebra*

2. *Z(G) has finite index in G*

3. *G′ has finite order which is invertible in R.*

PROOF. See [3]. ∎

3.2 Skew group ring

As in the case of a Galois extension, we often encounter situations of a **group action**, in which a group acts on a ring A by automorphisms. Formally one has a group homomorphism

$$\varphi : G \longrightarrow \mathrm{Aut}_K(A)$$

where $\mathrm{Aut}_K(A)$ denotes the group of K-linear automorphisms of A if A is an algebra over a commutative ring K. Note that φ does not have to be injective. For simplicity we denote $\varphi(g)(a)$ by $g \cdot a$ (although often in the literature ${}^g a$ or a^g is used).

Let A be a K-algebra with group action by G. Then we can form its **skew group ring** which is the free left A-module $A * G$ with basis $\{\overline{g} \mid g \in G\}$ and multiplication defined as

$$(a_g \overline{g})(b_h \overline{h}) = a_g (g \cdot b_h) \overline{gh}$$

for all $a_g, b_h \in A$ and $g, h \in G$.

$A * G$ becomes an associative K-algebra with unit $1\overline{e}$.

If G acts trivially on A, that is if $\varphi : G \to \mathrm{Aut}_K(A)$ sends any element to the indentity map of A, i.e. $\varphi(a) = id$. Then the above multiplication becomes the multipliction of the group ring, i.e. $A * G = A[G]$ in this case.

A is a left $A * G$-module by the following action:

$$a\overline{g} \cdot x = a(g \cdot x)$$

for all $a, x \in A$ and $g \in G$. Note that we assume that automorphisms respect the unit element. Hence $g \cdot 1_A = 1_A$ for all $g \in G$.

Also here we have a surjective $A * G$-linearmap from $A * G$ onto A defined by

$$\alpha : A * G \to A, \quad a\overline{g} \mapsto a\overline{g} \cdot 1 = a.$$

Here α is in general not a ring homomorphism unless the action of G is trivial, since for all $a \in A$ and $g \in G$

$$\alpha((1\overline{g})(a\overline{e})) = \alpha((g \cdot a)\overline{e}) = g \cdot a$$

while

$$\alpha(1\overline{g})\alpha(a\overline{e}) = 1a = a$$

However Lemma 3.2 also holds for group actions as an inspection of its proof shows:

Lemma 3.13 *If $\mathcal{G}$ is a set of group generators of G, then*

$$A = \mathrm{Ker}(\alpha : A * G \to A) = \sum_{g \in \mathcal{G}} A * G(1 - \overline{g}).$$

This also allows again to conclude that A is finitely presented as $A * G$-module if G is a finitely generated group.

As the center of an algebra A is isomorphic to its endomorphism as A^e-module, the endomorphism ring of A as $A * G$-module is also isomorphic to a subring of A, the fixring:

$$A^G = \{a \in A \mid \forall g \in G : g \cdot a = a\}$$

The we have a ring isomorphism

$$\phi : \mathrm{End}_{A*G}(A) \longrightarrow A^G$$

given by

$$f \mapsto phi(f) = (1)f$$

Because for any $f, g \in \mathrm{End}_{A*G}(A)$ one has

$$\phi(f \circ g) = ((1)f)g = (1)f(1)g = \phi(f)\phi(g).$$

Hence $A^G \simeq \mathrm{End}_{A*G}(A)$. Moreover for any left $A*G$-module M we define: $M^G = \{m \in M \mid \forall g \in G; g \cdot m = m\}$ Then we have a left A^G-isomorphism

$$\mathrm{Hom}_{A*G}(A, M) \longrightarrow M^G$$

given by $f \mapsto (1)f$. One can show that this isomorphism is functorial, i.e. $\mathrm{Hom}_{A*G}(A, -)$ is isomorphic $(-)^G$ as a functor from $A*G-\mathrm{Mod}$ to $A^G-\mathrm{Mod}$..

The conclusion that a non-zero homomorphism $R \to R[G]$ implies that G is finite also holds for skew group rings:

Lemma 3.14 *If there exists $0 \neq f \in \mathrm{Hom}_{A*G}(A, A*G) \neq 0$, then G is finite and there exists $a \in A$ such that*

$$(1)f = \sum_{g \in G} (g \cdot a)\overline{g}.$$

Proof. Let $f : A \to A*G$ be a non-zero $A*G$-linear map, then $(a)f = a(1)f$ for all $a \in A$. Let $(1)f = \sum_{h \in H} a_h \overline{h}$ and $0 \neq a_h \in A$ for all $h \in H$ where $H = supp(f(1))$. For any $g \in G$ we have

$$\sum_{h \in H} a_h \overline{h} = (1)f = (g \cdot 1)f = \overline{g}(1)f = \sum_{h \in H} (g \cdot a_h)\overline{gh} = \sum_{k \in gH} ((g^{-1}k) \cdot a_{g^{-1}k})\overline{k}, \tag{3.2}$$

i.e. $gH = H$ for any $g \in G$. Thus $G = H$ and hence G is finite. Furthermore by (3.2) $(g^{-1}k) \cdot a_{g^{-1}k} = a_k$ for any $g \in G$, i.e. $g^{-1} \cdot a_{g^{-1}} = a_e =: a$ for any $g \in G$. or equivalently

$$a_g = g \cdot a_e \quad \forall g \in G.$$

Thus $(1)f = r \sum_{g \in G} (g \cdot a)\overline{g}$. ∎

Definition 3.15 *Let G be a finite group acting on A. The trace of an element a is defined to be*

$$\mathrm{tr}_G(a) = \sum_{g \in G} (g \cdot a).$$

Note that the trace is a map $\mathrm{tr}_G : A \longrightarrow A^G$, because for any $h \in G, a \in A$, we have

$$h \cdot tr_G(a) = \sum_{g \in G} h \cdot (g \cdot a) = \sum_{g \in G} (hg) \cdot a = \sum_{g \in G} g \cdot a = tr_G(a).$$

Theorem 3.16 *The following statements are equivalent:*

(a) A is a projective left $A*G$-module;

(b) G is finite and $\exists a \in A$ such that $\sum_{g \in G} g \cdot a = 1$;

(c) G is finite and $tr : A \to A * G$ is surjective.

PROOF. $(a) \Rightarrow (b)$ we already saw that G has to be finite. Moreover there exists a map $f : A \to A * G$ which splits α, i.e.

$$1 = ((1)f)\alpha = \sum_{g \in G} (g \cdot a) = tr_G(a)$$

for some $ainA$.

$(b) \Leftrightarrow (c)$ is clear.

$(b) \Rightarrow (a)$ note if G is finite, then for any $a \in A$ the map $f : A \to A * G$ with

$$(x)f = \sum_{g \in G} x\overline{g}(a\overline{e}) = \sum_{g \in G} x(g \cdot a)\overline{g}$$

is $A * G$-linear. Since $((1)f)\alpha = \sum_{g \in G}(g \cdot a) = \mathrm{tr}(_)G(a)$ we are done. ∎

Remark 3.17 *Note that in the group ring case, the action is trivial. Hence condition (b) says that there exists an element $a \in A$ such that*

$$\sum_{g \in G} (g \cdot a) = \sum_{g \in G} a = |G|a = 1$$

which is equivalent to say that $|G|$ is invertible in A. The following example however shows that A might be a projective left $A * G$-module without $|G|$ being invertible in A:

Example 3.18 *Take any field K and $A = K \times K$. Define the automorphism $\gamma(a, b) = (b, a)$ for all $(a, b) \in A$ and let $G = \langle \gamma \rangle$ the subgroup of $Aut(A)$ of order 2 generated by γ. Then A contains an element of trace one, namely $x = (1, 0)$, because $x + g \cdot x = (1, 0) + (0, 1) = (1, 1)$. Hence A is a projective left $A * G$-module. On the other hand $|G|$ is invertible in A if and only if $char(K) \neq 2$.*

It also follows from 3.16 that G is finite provided $A \subseteq A * G$ is separable. Here we give a necessary condition for $A \subseteq A * G$ to be separable.

Theorem 3.19 *Let G be a finite group acting on a K-algebra A such that A has a central element of trace 1. Then $A \subseteq A * G$ is separable.*

PROOF. Let $a \in Z(A)$ with $\mathrm{tr}(a) = 1$ and set

$$e = \sum_{g \in G} \overline{g} \otimes_A a\overline{g^{-1}} \in (A * G) \otimes_A (A * G).$$

Then applying the multiplication we get

$$\mu(e) = \sum_{g \in G} (g \cdot a)\overline{gg^{-1}} = \mathrm{tr}(a)\overline{e} = 1_{A*G}.$$

For any $x \in A$

$$\begin{aligned} xe &= \sum_{g \in G} x\overline{g} \otimes_A a\overline{g^{-1}} \\ &= \sum_{g \in G} \overline{g}(g^{-1} \cdot x)\overline{e} \otimes_A a\overline{g^{-1}} \\ &= \sum_{g \in G} \overline{g} \otimes_A (g^{-1} \cdot x)\overline{e}a\overline{g^{-1}} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{g\in G} \overline{g}\otimes_A (g^{-1}\cdot x)\overline{ag^{-1}} \\
&= \sum_{g\in G} \overline{g}\otimes_A \overline{ag^{-1}}(g\cdot(g^{-1}\cdot x)\overline{e} \\
&= \sum_{g\in G} \overline{g}\otimes_A \overline{ag^{-1}}x\overline{e} = ex
\end{aligned}
$$

where we use the fact in the 5. line that a is central.

For any $h \in G$ we have:

$$
\begin{aligned}
\overline{he} &= \sum_{g\in G} \overline{h}\overline{g}\otimes_A \overline{ag^{-1}} \\
&= \sum_{g\in G} \overline{hg}\otimes_A \overline{ag^{-1}} \\
&= \sum_{k\in hG} \overline{k}\otimes_A \overline{a(h^{-1}k)^{-1}} \\
&= \sum_{k\in hG} \overline{k}\otimes_A \overline{ak^{-1}}\overline{h} = e\overline{h}
\end{aligned}
$$

Thus e is a separability idempotent of $A*G$ over A. ∎

Note that if $|G|$ is invertible in A, then $\frac{1}{|G|}$ is a central element of trace one.

Corollary 3.20 *If $|G|$ is invertible in A then $A \subseteq A*G$ is separable.*

Theorem 3.19 also shows that forr any commutative K-algebra A with group action G, $A \subseteq A*G$ is separable if and only if there exists an element of trace one. Note that the Example 3.18 is commutative, so the extension $A \subseteq A*G$ is separable although $|G|$ is not invertible in A.

Open questions: Find sufficient and necessary conditions for $A*G$ to be semisimple artinian or von Neumann regular.

Theorem 3.21 (Alfaro-Ara-delRio) *If $A*G$ is von Neumann regular then*

1. *$A*H$ is von Neumann regular for all subgroups $H \subseteq G$;*
2. *G is locally finite*
3. *for any finite subgroup H of G, there exists an element a of trace 1, i.e. $\mathrm{tr}_H(a) = 1$.*

Proof. Note that (2) and (3) follow from (1), because if $A*H$ is von Neumann regular for a finitely generated subgroup H of G, then $K = \mathrm{Ker}(\alpha : A*H \to A)$ is a finitely generated left ideal of $A*H$ by Lemma 3.13. Hence A is finitely presented and thus projective as $A*H$-module which implies (2) and (3) by Theorem 3.16. (1) is proved as in the group ring case: take $\gamma = \sum_{h\in H} a_h\overline{h} \in A*H$. Then there exist $\gamma' = \sum_{g\in G} b_g\overline{g}$ such that $\gamma = \gamma\gamma'\gamma$, i.e.

$$
\sum_{h\in H} a_h\overline{h} = \left(\sum_{h\in H} a_h\overline{h}\right)\left(\sum_{g\in G} b_g\overline{g}\right)\left(\sum_{k\in H} a_k\overline{h}\right) = \left(\sum_{h,k\in H, g\in G} a_h h\cdot(b_g(g\cdot a_k))\overline{hgk}\right)
$$

Note that $hkg \in H$ for $h,k \in H$ if and only if $g \in H$. Thus (by comparing coefficients) we have that

$$
\sum_{h,k\in H, g\notin H} a_h h\cdot(b_g(g\cdot a_k))\overline{hgk} = 0.
$$

Set $\gamma'' = \sum_{g\in H} b_g\overline{g} \in A*H$ we have $\gamma = \gamma\gamma''\gamma$, i.e. $A*H$ is regular. ∎

Combining with 3.19 we have that for a commutative ring A, $A*G$ is von Neumann regular if and only if $A \subseteq A*G$ is locally separable and A is von Neumann regular.

Corollary 3.22 *Let A be a K-algebra with K of characteristic 0 and G a group.*

1. *$A * G$ is semisimple if and only if G is finite and A is semisimple*
2. *$A*G$ is von Neumann regular if and only if G is locally finite and A is von Neumann regular.*

PROOF. Since $char(K) = 0$, any order of a finite group will be invertible in K.
(2) Suppose that G has to be locally finite and A is regular. Since any element of $A * G$ is contained in a subring $A * H$ with H being finite whose order is invertible by the assumption of the characteristic, $A \subseteq A * H$ is separable, i.e. $A \subseteq A * G$ is locally separable and by 3.9 $A * G$ is regular. The converse follows from Theorem 3.21. ∎

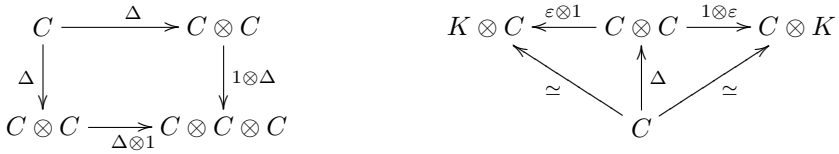
Chapter 4

Hopf algebra actions

For simplicity we will only deal with algebras over fields K.

4.1 Hopf algebras

Definition 4.1 *A coassociative coalgebra with counit is a K-vector space C with K-linear maps $\Delta : C \longrightarrow C \otimes C$ (comultiplication) and $\varepsilon : C \longrightarrow K$ (counit), such that the following diagrams are commutative:*



We will use the so-called Sweedler-notation for the comultiplication of an element c:

$$\Delta(c) = \sum_{(c)} c_1 \otimes c_2.$$

Is C a K-coalgebra and A a K-algebra, then $\mathrm{Hom}_K(C, A)$ becomes a K-algebra by the **convolution product**: $\forall f, g \in \mathrm{Hom}_K(C, A)$ we set $(f \star g)(c) := \sum_{(c)} f(c_1)g(c_2)$ for all $c \in C$. If ε is the counit of C and $\eta : K \to A$ the unit of A, then $\eta \circ \varepsilon \in \mathrm{Hom}_K(C, A)$ is the unit of this algebra. In particular $C^* = \mathrm{Hom}_K(C, K)$ is a K-algebra with unit ε.

Definition 4.2 *A K-algebra B is called K-***Bialgebra** *if B is a K-coalgebra such that the comultiplication and counit are algebra maps. A K-bialgebra H is called* **Hopfalgebra**, *if the identity $id \in \mathrm{End}_K(H)$ has an inverse S w.r.t. the convolution product. S is called the antipode of H. and one has*

$$\sum_{(h)} h_1 S(h_2) = \varepsilon(h) = \sum_{(h)} S(h_1)h_2.$$

Example 4.3 *We list some examples of Hopf algebras*

1. *$K[G]$ is a Hopf algebra with $\Delta(\overline{g}) = \overline{g} \otimes \overline{g}$ and $\epsilon(\overline{g}) = 1$ and $S(\overline{g}) = \overline{g^{-1}}$ for all $g \in G$.*
2. *Let $\mathfrak{g}$ be a Lie algebra over K, i.e. there exists a bilinear form*

$$[,] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$$

such that $[x, y] = -[y, x]$ and

$$[x, [y, z]] + [y, [z, x]] + [z, [y, x]] = 0$$

for all $x, y, z \in \mathfrak{g}$. *Let* $H = U(\mathfrak{g})$ *be its envelopping algebra, i.e.*

$$U(\mathfrak{g}) = T(\mathfrak{g})/\langle x \otimes y - y \otimes x - [x, y] \rangle$$

for all $x, y \in \mathfrak{g}$. *Then* H *is a Hopf algebra with*

$$\Delta(x) = 1 \otimes x + x \otimes 1$$

for all $x \in \mathfrak{g}$ *and* $\epsilon(x) = 0$ *and* $S(x) = -x$.

3. *Let* G *be an algebraic group and* $H = \mathcal{O}(G)$ *its coordinate ring. Then*

$$\begin{array}{ll} \Delta : \mathcal{O}(G) \to \mathcal{O}(G \times G) \simeq \mathcal{O}(G) \times \mathcal{O}(G) & f \mapsto [(g, h) \mapsto f(gh)] \\ \epsilon : \mathcal{O}(G) \to K & \epsilon(f) = f(1) \\ \epsilon : \mathcal{O}(G) \to \mathcal{O}(G) & f \mapsto [g \to f(g^{-1})] \end{array}$$

K is also a left H-module. For any left H-module M we define:

$$M^H = \{m \in M \mid \forall h \in H : h \cdot m = \epsilon(h)m\}.$$

As in the group action case we have an K-isomorphism:

$$\mathrm{Hom}_H(K, M) \longrightarrow M^H$$

$$f \mapsto f(1)$$

which is actually a functorial isomorphism between $\mathrm{Hom}_H(K, -)$ and $(-)^H$.

As in the group ring case one can show:

Lemma 4.4 *If* $\mathrm{Hom}_H(K, H) \neq 0$ *then* H *is finite dimensional and there exists* $0 \neq t \in H$ *such that for any* $f \in \mathrm{Hom}_H(K, H)$ *there exists* $\lambda \in K$ *with* $f(1) = \lambda t$.

The element t is called a left integral and is characterised by the property that for all $h \in H$: $ht = \epsilon(h)t$.

Theorem 4.5 *The following statements are equivalent for a Hopf algebra* H *over a field* K*:*

1. H *is separable over* K*;*
2. H *is a semisimple artinian* K*-algebra;*
3. $(-)^H$ *is an exact functor;*
4. *there exists a non-zero left integral* $t \in H$ *such that* $\epsilon(t) = 1$.

In this case H *is finite dimensional.*

One says that a Hopf algebra H acts on a K-algebra A if there exists a K-linear map

$$\cdot : H \otimes A \longrightarrow A$$

that turns A into a left H-module such that the multiplication and the unit are H-linear, i.e.

1. $h \cdot (ab) = \sum_{(h)} (h_1 \cdot a)(h_2 \cdot b)$
2. $h \cdot 1 = \epsilon(h)1$.

We have also here constructions similar to the one seen before:

1. The smash product of A and H is the K-vector space $A\#H = A \otimes_K H$ with multiplication

$$(a\#h)(b\#g) = \sum_{(h)} a(h_1 \cdot b)\#h_2 b.$$

2. Again A is a left $A\#H$-module by $a\#h\cdot x = a(h\cdot x)$ and there exists a surjective $A\#H$-linear map
$$\alpha : A\#H \to A \quad \alpha(a\#h) = a\epsilon(h).$$

3. The endomorphism ring of A as $A\#H$-module is isomorphic to A^H:
$$\mathrm{End}_{A\#H}(A) \to A^H \quad f \mapsto f(1).$$

4. The functors $\mathrm{Hom}_{A\#H}(A,-)$ and $(-)^H$ from $A\#H$-Mod to A^H-Mod are isomorphic.

Corollary 4.6 *Let H be a semisimple Hopf algebra over k. Then for any H-module algebra A: $A \subseteq A\#H$ is a separable extension.*

Corollary 4.7 *Let H be a semisimple Hopf algebra over k and A a H-module algebra.*

1. *A semisimple artinian $\Rightarrow$ $A\#H$ semisimple artinian*
2. *A von Neumann regular $\Rightarrow$ $A\#H$ von Neumann regular.*

Bibliography

[1] R.Alfaro, P.Ara, A. Del Rio, "Regular Skew Group Rings", Journal of the Australian Mathematical Society Ser A 58 (1995), 167-182

[2] M.Auslande, O.Goldman, "The Brauer Group over a commutative ring", Transaction AMS 97(3) 1960, 367-409

[3] F.R.DeMeyer, G.J.Janusz, "Group rings which are Azumaya", Transaction AMS 279(1) 1983, 389-395

[4] B.Farb, R.K.Dennis, "Noncommutative Algebra", Springer GTM 144 (1993)

[5] I.N. Herstein, "Noncommutative Rings", The Carus Math. Monographs 15 (1973)

[6] K.Hirata, K.Sugano, "on semisimple extensions and separable extensions over non commutative rings", J. Math. Soc. Japan 18(4) 360-373 (1966) `http://www.journalarchive.jst.go.jp/jnlpdf.php?cdjournal=jmath1948&cdvol=18&noissue=4&startpage=360&lang=en&from=jnltoc`

[7] H.J.Schneider, "Lectures on Hopf algebras", Trabajos de Matemtica 31/95. Universidad Nacional de Cordoba `http://www.mate.uncor.edu/andrus/papers/Schn1.dvi.gz`

[8] R.Wisbauer, "Foundations in Module and Ring Theory", Gordon Breach (1991)

[9] R.Wisbauer, "Modules and algebras: bimodule structure and group actions on algebras", Longman (1996)