Notes for the Geometry of division algebras

Danny Krashen

June 14, 2024

Contents

Introduction

Our first goal will be to try to understand the structure and classification of finite dimensional division algebras over fields. Perhaps this subject starts with William Rowan Hamilton's famous discovery of the quaternions in 1843.

Brief history and context

- discovery and historical context of the quaternions
- other systems – octonions, clifford algebras
- frobenius' theorem
- resurgence around 1900 with Dickson, Wedderburn, etc
- ABHN theorem and class field theory
- dry spell until 50's
- 50's: Amitsur's noncrossed products, generic splitting fields, Chatelet's varieties, Borel's classification of "classical groups"
- 60's: Auslander, Goldman and separability, then Grothendieck, then Giraud's gerbes
- 70's: PI algebras and huge increase in activity, conferences

Chapter 1

Background on rings and modules

In this chapter we will develop the basic structure theory of finite dimensional simple rings (i.e. Wedderburn's structure theorem) together with some standard useful results for working with central simple algebras, such as the double centralizer theorem and the Noether-Skolem theorem. The basic tool we will use is the interplay the structure of rings and of their categories of modules. From this perspective, a natural first goal will be the Morita theorems, which tell us when module categories of two different rings may be equivalent.

We will start with a few basic ring-theoretic preliminaries.

1.1 Ring preliminaries

1.1.1 Simple and semisimple rings

Our strategy for developing some structure theory of rings will be primarily via understanding their interactions with modules. On the one hand, given a ring R and a left R-module M, we obtain a natural ring map $R \to \mathrm{End}(M)$, where the right hand side is the ring of endomorphisms considering M as an Abelian group. In the case that R has the structure of an algebra over some commutative ring k, we similarly get a homomorphism $R \to \mathrm{End}_k(M)$. While this is interesting in the context of understanding our ring in terms of, for example, matrices in the case that k is a field and M is finite dimensional, we obtain much more information by considering some additional structure on the module M as we now describe.

For an R-module M, we will want to consider the R-linear endomorphisms of M, which forms a ring $S = \mathrm{End}_R(M)$. We see that M now has two compatible module structures as both a left R-module and as a left S-module and that these

operations are compatible in the sense that

$$r(sm) = s(rm) \quad \forall r \in R, s \in S, m \in M,$$

from the fact that S acts as R-linear maps. As our rings are potentially non-commutative, many authors choose to work instead with right instead of left R-modules for such discussions. That is, if N is a right R-module and S is ring of right R-linear endomorphisms of N, the analog of the above equation is the identity

$$s(nr) = (sn)r \quad \forall r \in R, s \in S, n \in N,$$

which turns the prior "commutativity" relation into an "associativity" relation. While this is a handy convention, we will mostly not use it in this section and stick to considering only left R-modules.

In any case, it is now automatic that for a (left) R-module M, if we set $S = \mathrm{End}_R(M)$, then reading our relation in reverse shows us that R acts on M as S-linear endomorphisms, giving us a map

$$R \to \mathrm{End}_S(M),$$

and in favorable circumstances, understanding aspects of the structure of S and M will then give strong information about R.

Definition 1.1.1. Let R be a ring and M a left R-module. We say that M is simple if $M \neq 0$ and the only submodules of M are 0 and M. We say that a module is semisimple if it is a direct sum of simple modules.

Definition 1.1.2. Let R be a k-algebra and M a left R-module. For $m \in M$, we define the (left) annihilator of m to be the set of $r \in R$ such that $rm = 0$. We note that this is a left ideal of R.

Definition 1.1.3. Let R be a k-algebra and M a left R-module. We define the (left) annihilator of M, denoted $\mathrm{ann}_R(M)$ (or as $\mathrm{l.ann}_R(M)$ if we need to be clear to distinguish left from right modules) to be the ideal of R consisting of those $r \in R$ such that $rm = 0$ for all $m \in M$. Note $\mathrm{ann}_R(M) = \bigcap_{m \in M} \mathrm{ann}_R(m)$ and that this is a two-sided ideal of R.

Of course, we define right annihilators analogously.

Definition 1.1.4. Let R be a ring and M a left R-module. We say that M is faithful if $\mathrm{ann}_R(M) = 0$.

Note that if M is a faithful R-module we obtain an injective map $R \to \mathrm{End}_k(M)$. Consequently, one nice use of faithful modules is that they give concrete realizations of our algebras R. For example, if k was a field, this would exhibit R as an algebra of matrices over k.

Lemma 1.1.5. *Let R be a ring and M a left R-module. Then the following are equivalent:*

1. *M is faithful,*

2. *$M^{\oplus I}$ is faithful for some index set I,*

3. *there exists a submodule $N \subset M$ such that N is faithful.*

Definition 1.1.6. Let R be a ring. We define the Jacobson radical $J(R)$ of R to be the intersection of all maximal left ideals of R. We say that R is semiprimitive if $J(R) = 0$.

Lemma 1.1.7. *Let R be a ring. Then $J(R)$ is a two-sided ideal of R and can be described as*

$$J(R) = \bigcap_{\substack{M \text{ simple left} \\ R\text{-module}}} ann_R(M).$$

This is a straightforward consequence of the following Lemma:

Lemma 1.1.8. *Let R be a ring and M a left R-module. Then the following are equivalent:*

(1) for every $m \in M \backslash \{0\}$, $\operatorname{ann}_R(m)$ is a maximal left ideal of R,

(2) for some $m \in M$, $\operatorname{ann}_R(m)$ is a maximal left ideal of R,

(3) $M \cong R/J$ for some maximal left ideal $J \subseteq R$,

(4) M is a simple left R-module.

Proof. Clearly (1) implies (2). If (2) holds, we find that by simplicity $M = Rm$ and so the natural map $R \to M$ given by $r \mapsto rm$ is surjective, which implies $M \cong R/\operatorname{ann}_R(m)$, showing (3) with $J = \operatorname{ann}_R(m)$. If (3) holds, then (4) follows immediately from the correspondence theorem. Finally, if (4) holds and $m \in M$ is nonzero then Rm is a nonzero submodule and hence must be M. It follows that we have an isomorphism $R/\operatorname{ann}_R(m) \cong M$ and so $\operatorname{ann}_R(m)$ is a maximal left ideal as claimed. □

While this definition would seem to leave open the possibility of there being a different notion of a right Jacobson radical, as we will see, this notion is in fact "ambidextrous."

Definition 1.1.9. Let R be a ring. We say that $r \in R$ is right (resp. left) quasiregular if $1 - r$ has a right (resp. left) inverse. We say that r is quasiregular if it is both left and right quasiregular.

We recall that in a ring R, an element $r \in R$ having a left multiplicative inverse need not imply r has a right inverse and conversely. On the other hand, let us recall a few elementary facts about when one sided inverses and two sided inverses concide.

Lemma 1.1.10. *Let R be a ring and suppose $r \in R$ has both a right an a left multiplicative inverse, say $ar = 1 = rb$. Then $a = b$.*

Proof. This follows from the elementary computation $b = 1b = arb = a1 = a$. □

Lemma 1.1.11. *Let R be a ring and suppose $a, r \in R$ with $ar = 1$. If a also has a left inverse then $ra = 1$.*

Proof. Suppose $b \in R$ with $ba = 1$. Then by Lemma 1.1.10, we have $b = r$. But therefore $ra = ba = 1$. □

Lemma 1.1.12 (Isaacs, Thm. 13.4)**.** *Let R be a ring. Then every element of $J(R)$ is quasiregular.*

Proof. Let $r \in J(R)$. We first show that r is left quasiregular. For this, consider the left ideal $R(1-r)$ generated by $1-r$. We claim $R(1-r) = R$, which would say that r is left quasiregular. Arguing by contradiction, if $R(1-r) \neq R$ then we may choose I a maximal left ideal containing $R(1-r)$. Since $r \in J(R)$ it is in every maximal right ideal and so $r \in I$. But $1 - r \in M$ by construction which gives the contradiction $1 \in M$.

We now show that r is right quasiregular. As is already left quasiregular, we may write $s(1-r) = 1$. By Lemma 1.1.11, it suffices to show that s has a left inverse. For this, we consider $y = 1 - s$ and note that as $s = 1 - y$, s having a left inverse is the same as y being left quasiregular. Consequently it suffices to show that $y \in J(R)$. But for this, we write

$$1 = s(1-r) = (1-y)(1-r) = 1 - y - r + yr$$

and so $yr - y - r = 0$ which gives $y = (y-1)r$ and $r \in J(R)$ tells us that $y \in J(R)$, completing the proof. □

Theorem 1.1.13 (Isaacs, Thm. 13.4)**.** *Let R be a ring. Then $J(R)$ is the largest two-sided ideal consisting of quasiregular elements.*

It follows from this that the "right" and "left" Jacobson radicals coincide.

Proof. In fact, we will show that if I is any left ideal consisting of left quasiregular elements, then $I \subseteq J(R)$. For this, suppose we have such an ideal I. It suffices to show that $I \subseteq M$ for every maximal left ideal M. Choosing such a maximal M, if $I \nsubseteq M$ then as M is maximal, we have $I + M = R$ and so we may write $1 = x + m$ for $x \in I, m \in M$, and so $m = 1 - x$. But as $x \in I$ is left quasiregular, this implies m is left invertible, contradicting the fact that M is a proper ideal. □

Theorem 1.1.14 (Nayakama's Lemma, Rowen's Ring theory, Prop 2.5.24)**.** *Let R be a ring and $M \neq 0$ a finitely generated left R-module. Then $J(R)M \neq M$.*

Proof. Choose $m_1, \ldots, m_n \in M$ a minimal generating set. If $J(R)M = M$ we may write $m_n = \sum_{i=1}^{n} x_i m_i$ for $x_i \in J(R)$. Subtracting, we find $(1 - x_n)m_n = \sum_{i=1}^{n-1} x_i m_i$. But $x_n \in J(R)$ is quasiregular and hence $(1 - x_n)$ has some inverse, say $a \in R$. But therefore we find $m_n = \sum_{i=1}^{n-1} (ax_i)m_i$, showing that m_n is in the span of $m_1, \ldots, m_{n-1}$ and contradicting the minimality of our generating set. □

1.2 The Morita theorems and double centralizers

The Morita theorems function by a very useful mechanism that we will see in various contexts. We can refer to this as the double centralizer phenomena, which occurs when we have a k-algebra A (for some commutative ring k), a subalgebra $B \subseteq A$, and we consider the centralizer $\mathrm{C}_A(B)$. It is a tautology that we have an inclusion

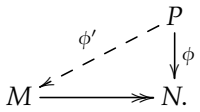
$$B \subseteq \mathrm{C}_A(\mathrm{C}_A(B)).$$

We will find that in favorable circumstances, we actually have an equality. When this happens, it will often reflect an interesting relationship between these three algebras.

In understanding the structure theory of k-algebras, we will see that the matrix algebra $\mathrm{M}_n(k)$ will turn out to play a role of a kind of trivial algebra. This will be first reflected as a consequence of Morita theory (see **??**), where we will see that both k and $\mathrm{M}_n(k)$ have equivalent categories of modules.

1.2.1 Projectives and generators

Definition 1.2.1. Let R be a ring and P a left R-module. We say that P is projective if for every surjective map of R-modules $M \twoheadrightarrow N$ and every homomorphism $\phi : P \to N$, there exists $\phi' : P \to M$ giving a commutative diagram



Lemma 1.2.2. *The following are equivalent for a left R-module P*

1. *P is projective,*
2. *there exists an R-module P' such that $P \oplus P' \cong R^{\oplus I}$ for some index set I.*

Furthermore, we can choose I to be finite if P is finitely generated.

Proof. If P is projective, choose a surjection $R^{\oplus I} \to P$ via a generating set of cardinality $|I|$. By hypothesis, the identity map $P \to P$ lifts to a map $P \to R^{\oplus I}$ and hence the surjection is split, giving $R^{\oplus I} \cong P \oplus P'$ where P' is the kernel of the map $R^{\oplus I} \to P$. Conversely, if $P \oplus P' \cong R^n$, $M \twoheadrightarrow N$ is a surjection and $\phi : P \to N$ is any morphism, consider the morphism $\widetilde{\phi} : R^n \to N$ given by the composition $R^n \cong P \oplus P' \to P \xrightarrow{\phi} N$. It suffices to show that $\widetilde{\phi}$: can be lifted to a map to M. But as $\mathrm{Hom}_R(R^{\oplus I}, M) = \mathrm{Map}(I, M)$ and $\mathrm{Hom}_R(R^{\oplus I}, N) = \mathrm{Map}(I, N)$ this just amount to lifing the set map (corresponding to our free generators). □

Note that as a trivial consequence, R is projective, as is any free module $R^{\oplus I}$.

Definition 1.2.3. Let R be a ring and M a left R-module. We say that M is a generator if for every other left R-module N, there exists a surjective map $M^{\oplus I} \twoheadrightarrow N$.

Interestingly, generators have a somewhat "dual" characterization as compared to projectives:

Lemma 1.2.4 (Anderson and Fuller, 17.6)**.** *Let R be a ring and M a left R-module. Then the following are equivalent*

1. *M is a generator,*
2. *there exists a left R-module Q such that $M^n \cong R \oplus Q$ for some $n \in \mathbb{N}$.*

Proof. As M is a generator, we can find some I and some surjective map $\phi : M^{\oplus I} \to R$. Choose $m \in M^{\oplus I}$ with $\phi(m) = 1$. As every element in $M^{\oplus I}$ lies in a finite sub-direct sum, we can choose some finite subset $I_0 \subset I$ such that $m \in M^{\oplus I_0} \subset M^{\oplus I}$. But then the restriction $\phi_0 : M^{\oplus I_0} \to R$ has 1 in its image and hence is surjective. Without loss of generality, we may assume we have a surjection $\phi : M^n \to R$. But as R is projective, we obtain a direct sum $M^n \cong R \oplus Q$ where $Q = \ker(\phi)$. □

Another "dual" type statement relating generators and projectives is as follows:

Proposition 1.2.5. *Let R be a ring and M an R-module. Let $S = \mathrm{End}_R(M)$. Then we may consider M as either an R-module or as an S-module.*

(1) if M is a finitely generated projective R-module then it is a generator as an S-module,

(2) if M is a generator as an R-module, then it is finitely generated and projective as an S-module.

Proof. For (1), suppose M is finitely generated and projective and choose M' so that $M \oplus M' \cong R^n$. Then as S-modules, we have an identification:

$$M^{\oplus n} = \mathrm{Hom}_R(R^{\oplus n}, M) = \mathrm{Hom}_R(M \oplus M', M) \cong \mathrm{End}_R(M) \oplus \mathrm{Hom}_R(M', M),$$

and so setting $Q = \mathrm{Hom}_R(M', M)$, we find $M^{\oplus n} \cong S \oplus Q$, showing that M is a generator by Lemma 1.2.4.

For (2), we assume M is a generator over R and choose an R-module Q such that $M^{\oplus n} \cong R \oplus Q$. We then find that as S-modules we have:

$$S^{\oplus n} = \mathrm{End}_R(M)^{\oplus n} = \mathrm{Hom}_R(M^{\oplus n}, M) = \mathrm{Hom}_R(R \oplus Q, M) = M \oplus \mathrm{Hom}_R(Q, M),$$

which shows that M is a direct summand of the free module $S^{\oplus n}$ and is therefore projective. □

Lemma 1.2.6. *Let R be a ring and M a left R-module which is a generator. Then M is faithful.*

Proof. Writing $M^{\oplus n} \cong R \oplus Q$, we see that by Lemma 1.1.5 that M is faithful if and only if $M^{\oplus n}$ is faithful. But again by Lemma 1.1.5, this follows from the fact that $R \subset M^{\oplus n}$ is faithful. □

Definition 1.2.7. For a ring R, we say that a left R-module P is a progenerator if it is a finitely generated projective R-module which is a generator in the category of left R-modules.

1.2.2 Bi-endomorphisms and balanced modules

As we head towards double-centralizer type results, let us first make some observations about centralizers in matrix algebras. For notational convenience, let us make the following definition:

Definition 1.2.8. Let R be a ring and M an R-module. Let $S = \mathrm{End}_R(M)$. Then M is an S-module and we define $\mathrm{BiEnd}_R(M) = \mathrm{End}_S(M) = \mathrm{End}_{\mathrm{End}_R(M)}(M)$.

Note that we always have a canonical map $R \to \mathrm{BiEnd}_R(M)$.

Remark 1.2.9. Let R be a k-algebra for some commutative ring k and let M be an R-module. Then $\mathrm{End}_R(M)$ is a k-algebra. Repeating this logic, we see $\mathrm{End}_{\mathrm{End}(M)}(\mathrm{End}_R(M))$ is contained in $\mathrm{End}_k(M)$ and consequently $\mathrm{BiEnd}_R(M) = \mathrm{End}_{\mathrm{End}(M)}(\mathrm{End}_R(M)) = \mathrm{End}_{\mathrm{End}_k(M)}(End_R(M))$. That is, bi-endomorphism rings agree when computed either in terms of rings or in terms of k-algebras.

Remark 1.2.10. In the case that R is a k algebra for some commutative ring k and M is a faithful R-module, we have $R \subset \mathrm{End}_k(M)$, $\mathrm{End}_R(M) = \mathrm{C}_{\mathrm{End}_k(M)}(M)$ and $\mathrm{C}_{\mathrm{End}_k(M)}(\mathrm{C}_{\mathrm{End}_k(M)}(R)) = \mathrm{BiEnd}_R(M)$.

Definition 1.2.11. Let R be a k-algebra for some commutative ring k and let M be an R-module. We say that M is balanced if $R \to \mathrm{BiEnd}_R(M)$ is surjective and that M if faithfully balanced if this is an isomorphism (i.e. if M is faithful and balanced).

Lemma 1.2.12. *Let k be a commutative ring and R a k-algebra. Let M, N be R-modules and set $E = \mathrm{End}_k(M \oplus N)$. Then*

$$\mathrm{BiEnd}_R(M \oplus N) \subset \begin{bmatrix} \mathrm{BiEnd}_R(M) & 0 \\ 0 & \mathrm{BiEnd}_R(N) \end{bmatrix} \subset \begin{bmatrix} \mathrm{End}_k(M) & \mathrm{Hom}_k(N,M) \\ \mathrm{Hom}_k(M,N) & \mathrm{End}_k(N) \end{bmatrix} = E.$$

In particular we have a natural map $\mathrm{BiEnd}_R(M \oplus N) \to \mathrm{BiEnd}(M)$ which commutes with the natural maps $R \to \mathrm{BiEnd}_R(M \oplus N)$ and $R \to \mathrm{BiEnd}_R(M)$.

Proof. Let $e = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right] \in E$. We first show that any $T \in \mathrm{BiEnd}_R(M \oplus N)$ preserves the summand M in the decomposition $M \oplus N$ (and so by a similar argument for M, it preserves the full decomposition). For this, we check that $T(M \oplus 0) \subset M \oplus 0$, or equivalently $Te(M \oplus N) \subset e(M \oplus N)$. But this follows from the fact that $e \in \mathrm{End}_R(M \oplus N)$ and consequently $Te = eT$.

We therefore have $\mathrm{BiEnd}_R(M \oplus N) \subset \begin{bmatrix} \mathrm{End}_k(M) & 0 \\ 0 & \mathrm{End}_k(N) \end{bmatrix}$. But as the elements of $\mathrm{BiEnd}_R(M \oplus N)$ commute with the subring $\begin{bmatrix} \mathrm{End}_R(M) & 0 \\ 0 & \mathrm{End}_R(N) \end{bmatrix}$ of $\mathrm{End}_R(M \oplus N)$, it follow that $\mathrm{BiEnd}_R(M \oplus N) \subset \begin{bmatrix} \mathrm{BiEnd}_R(M) & 0 \\ 0 & \mathrm{BiEnd}_R(N) \end{bmatrix}$ as claimed. □

Lemma 1.2.13. *Let k be a commutative ring and R a k-algebra. Let N be an R-module. Then the natural map $R \to \mathrm{BiEnd}_R(R \oplus N)$ is surjective.*

Proof. Let $E = \mathrm{End}_k(R \oplus N)$. Suppose $\phi \in \mathrm{BiEnd}_R(R \oplus N) = \mathrm{C}_E(\mathrm{End}_R(R \oplus N))$.

For $n \in N$, consider the map $\lambda_n : R \to N$ with $\lambda_n(r) = rn$. We find $\lambda = \left[\begin{smallmatrix} 0 & \lambda_n \\ 0 & 0 \end{smallmatrix}\right] \in \mathrm{End}_R(R \oplus N)$ and if $T = \left[\begin{smallmatrix} r & 0 \\ 0 & \psi \end{smallmatrix}\right] \in \mathrm{BiEnd}_R(R \oplus N)$ (identifying $R = \mathrm{BiEnd}_R(R)$) then as $T\lambda = \lambda T$ we find $rn = \psi(n)$. Consequently ψ is the R-linear map given by $n \mapsto rn$ and so T is the image of the scalar multiplication by r map. □

Lemma 1.2.14. *Let $R \subset E$ be rings and let $S = \mathrm{C}_E(R)$. Then with respect to the diagonal inclusion of R, S, E into $M_n(E)$ as RI_n, SI_n, EI_n respectively, we have $\mathrm{C}_{\mathrm{M}_n(E)}(\mathrm{M}_n(R)) = S$ and $\mathrm{C}_{\mathrm{M}_n(E)}(S) = \mathrm{M}_n(R)$.*

We now come to our first version of a kind of double-centralizer theorem:

Lemma 1.2.15 (see Anderson and Fuller, Theorem 17.8)**.** *Let R be a ring and M an R-module which is a generator. Then M is faithfully balanced. In particular, if R is a k-algebra for some commutative ring k and $E = \mathrm{End}_k(M)$ then we have an inclusion $R \to E$ and the natural map $R \to \mathrm{C}_E(\mathrm{C}_E(R))$ is an isomorphism.*

Proof. Let $R' = \mathrm{C}_E(\mathrm{C}_E(R)) \subset \mathrm{End}_k(M)$. As M is faithful by Lemma 1.2.6, the natural map $R \to R'$ is injective. Write $M^n \cong R \oplus Q$ as in Lemma 1.2.4. We note that $\mathrm{End}_k(M^n) \cong \mathrm{M}_n(E)$. By Lemma 1.2.14 we have an identification $\mathrm{M}_n(\mathrm{C}_E(R)) = \mathrm{C}_{\mathrm{M}_n(E)}(R)$ and so

$$\mathrm{C}_{\mathrm{M}_n(E)}(\mathrm{C}_{\mathrm{M}_n(E)}(R)) = \mathrm{C}_{\mathrm{M}_n(E)}(\mathrm{M}_n(\mathrm{C}_E(R))) = \mathrm{C}_E(\mathrm{C}_E(R)) = R'.$$

But $\mathrm{C}_{\mathrm{M}_n(E)}(\mathrm{C}_{\mathrm{M}_n(E)}(R)) = \mathrm{BiEnd}_R(M^{\oplus n}) = \mathrm{BiEnd}_R(R \oplus Q)$. But by Lemma 1.2.13, the map $R \to R'$ is therefore surjective and hence an isomorphism. □

1.2.3 The Morita characterization of equivalences

Let R be a ring and suppose P is a progenerator. Consider the ring $S = \mathrm{End}_R(P)$. We see that we obtain a functor $\mathfrak{F}_P : R\text{-}\underline{\mathrm{mod}} \to S\text{-}\underline{\mathrm{mod}}$ via $M \mapsto P \otimes_R M$.

Theorem 1.2.16. *Let R and S be rings, and $F : R\text{-}\underline{\mathrm{mod}} \to S\text{-}\underline{\mathrm{mod}}$ is a functor. If F is an equivalence of categories then $F(R)$ is naturally an $S - R$ bimodule P which is an R^{op}-faithful S-progenerator such that $S = \mathrm{End}_{R^{op}}(P)$. Further, we have a natural isomorphism of functors $F \cong \mathfrak{F}_P$.*

Proof. Suppose F is an equivalence, and let $P = F(R)$. As F is an equivalence, it follows that P is projective and a generator since R is. We claim that P is finitely generated – for this, we note that for any index set I and surjective map $\oplus_{i \in I} M_i \to R$ in $R\text{-}\underline{\mathrm{mod}}$, the element $1 \in R$ is the image of some finite sum, and so we find that there is a finitely indexed sub-set $I_0 \subset I$ such that $\oplus_{i \in I_0} M_i \to R$ is still surjective. As this is a categorical property, it follows that P has the same property in the category $S\text{-}\underline{\mathrm{mod}}$. In particular, if we choose any generating set giving a surjection $S^{\oplus I} \to P$, we obtain a surjection from a finite sub-direct sum, showing that P is finitely generated. Hence P is an S-progenerator.

Consider the endomorphism ring $\mathrm{End}_S(P) = \mathrm{End}_{S\text{-}\underline{\mathrm{mod}}}(F(R))$. As we have an equivalence of categories, this is isomorphic to the endomorphism ring

$\mathrm{End}_R(R) = \mathrm{End}_{R\text{-}\underline{\mathrm{mod}}}(R) = R^{\mathrm{op}}$ (endomorphisms are given by right multiplication by elements of R). Consequently, P is an $S - R$ bimodule. Moreover, as any R-module map $f : R \to R$, necessarily induced by right multiplication by some $r \in R$ passes to, upon application of F a map $P \to P$ induced by this same multiplication, this time considering P as an R-module, we see that we can identify $F(f)$ with $P \otimes_R f$ (both being different descriptions of multiplication by r). More generally, as general maps $f : R^{\oplus I} \to R^J$ are combinations of these maps, we also see $F(f) = P \otimes_R f$ in this case as well.

As F is an equivalence, it preserves direct sums and exact sequences. In particular, if M is any R-module, we can choose a presentation

$$R^{\oplus I} \xrightarrow{f} R^J \longrightarrow M \longrightarrow 0,$$

and comparing the results of applying F, versus tensoring with P, we find we have a commutative diagram with exact rows (using that $F(f) = P \otimes_R f$):

$$\begin{array}{ccccccc} P^{\oplus I} & \xrightarrow{F(f)} & P^J & \longrightarrow & F(M) & \longrightarrow & 0 \\ \| & & \| & & & & \\ P^{\oplus I} & \xrightarrow{P \otimes_R f} & P^J & \longrightarrow & P \otimes_R M & \longrightarrow & 0. \end{array}$$

Therefore we obtain an isomorphism $F(M) \cong P \otimes_R M$. In Exercise 1.2.17 we check that these can fit together to produce a natural isomorphism $\alpha : F \to P \otimes_R \_$. $\square$

Exercise 1.2.17. *Show that choosing as in the proof of Theorem 1.2.16 a free resolution of each R-module M, we may obtain a natural isomorphism $\alpha : F \to P \otimes_R \_$.*

We also show that the converse of Theorem 1.2.16 holds. Before doing so, we record some preliminary lemmas:

Lemma 1.2.18. *Let R, S be rings, let P be a right R-module, let M be an $S - R$ bimodule, and let N be a left S-module. Consider the natural map $P \otimes_R \mathrm{Hom}_S(M, N) \to \mathrm{Hom}_S(\mathrm{Hom}_{R^{\mathrm{op}}}(P, M), N)$ given by $p \otimes f \mapsto (\phi \mapsto f(\phi(p)))$. If P is projective over R^{op}, then this is an isomorphism.*

Proof. Note that if $P \cong R^{\oplus I}$ is free, then this is just the identification

$$R^{\oplus I} \otimes_R \mathrm{Hom}_S(M, N) = \prod_I \mathrm{Hom}_S(M, N) = \mathrm{Hom}_S(M^{\oplus I}, N)$$
$$= \mathrm{Hom}_S(\mathrm{Hom}_{R^{\mathrm{op}}}(R^{\oplus I}, M), N),$$

verifying the claim in the case that P is free. In general, choose a right R-module P' with $R^{\oplus I} \cong P \oplus P'$ as right R-modules. By the naturality of this map in P, and right exactness of the tensor, we find we have a commutative diagram:

$$\begin{array}{ccccc} R^{\oplus I} \otimes_R \mathrm{Hom}_S(M, N) & \longrightarrow & P \otimes_R \mathrm{Hom}_S(M, N) & \longrightarrow & 0 \\ \| & & \downarrow & & \\ \mathrm{Hom}_S(\mathrm{Hom}_{R^{\mathrm{op}}}(R^{\oplus I}, M), N) & \longrightarrow & \mathrm{Hom}_S(\mathrm{Hom}_{R^{\mathrm{op}}}(P, M), N) & \longrightarrow & 0 \end{array}$$

which shows our map is surjective. Arguing similarly for P', we then find we have a commutative diagram

$$\begin{array}{ccccccc} 0 \to P' \otimes_R \mathrm{Hom}_S(M,N) & \longrightarrow & R^{\oplus I} \otimes_R \mathrm{Hom}_S(M,N) & \longrightarrow & P \otimes_R \mathrm{Hom}_S(M,N) & \longrightarrow & 0 \\ \downarrow & & \| & & \downarrow & & \\ \mathrm{Hom}_S(\mathrm{Hom}_{R^{\mathrm{op}}}(P',M),N) & \twoheadrightarrow & \mathrm{Hom}_S(\mathrm{Hom}_{R^{\mathrm{op}}}(R^{\oplus I},M),N) & \twoheadrightarrow & \mathrm{Hom}_S(\mathrm{Hom}_{R^{\mathrm{op}}}(P,M),N) & \twoheadrightarrow & 0 \end{array}$$

and a diagram chase now shows that the map

$$P \otimes_R \mathrm{Hom}_S(M,N) \to \mathrm{Hom}_S(\mathrm{Hom}_{R^{\mathrm{op}}}(P,M),N)$$

is injective and hence an isomorphism. □

Lemma 1.2.19. *Let R, S be rings, let P be a left S-module, let N be an $S-R$ bimodule, and let M be a left R-module. Consider the natural map $\mathrm{Hom}_S(P,N) \otimes_R M \to \mathrm{Hom}_S(P, N \otimes_R M)$ given by $f \otimes n \mapsto (p \mapsto f(p) \otimes n)$. If P is projective over S, then this is an isomorphism.*

Proof. This follows the same pattern as the proof of Lemma 1.2.18. □

Theorem 1.2.20 (Morita – see Anderson and Fuller 22.2)**.** *Let R be a ring and P a progenerator in R-$\underline{\mathrm{mod}}^{op}$. Let $S = \mathrm{End}_{R^{op}}(P)$. Then P is an $S-R$ bimodule and the morphism $\mathfrak{F}_P : R\text{-}\underline{\mathrm{mod}} \to S\text{-}\underline{\mathrm{mod}}$ given by $\mathfrak{F}_P(M) = P \otimes_R M$ is an equivalence of categories with inverse equivalence given by $\mathfrak{G}_P : S\text{-}\underline{\mathrm{mod}} \to R\text{-}\underline{\mathrm{mod}}$ via $\mathfrak{G}_P(N) = \mathrm{Hom}_S(P,N)$*[1]*.*

Proof. We check that these are inverse equivalences. For this we have (using Lemma 1.2.19) together with the fact that $R^{op} = \mathrm{BiEnd}_{R^{op}} P = \mathrm{End}_S(P)$ (i.e. $\mathrm{End}_S(P)$ can be identified with R acting by right multiplication):

$$\mathfrak{G}_P\mathfrak{F}_P(M) = \mathrm{Hom}_S(P, P \otimes_R M) = \mathrm{Hom}_S(P,P) \otimes_R M = R \otimes_R M = M.$$

For the other direction we have (using Lemma 1.2.18):

$$\mathfrak{F}_P\mathfrak{G}_P(N) = P \otimes_R \mathrm{Hom}_S(P,N) = \mathrm{Hom}_S(\mathrm{End}_{R^{op}}(P),N) = \mathrm{Hom}_S(S,N) = N.$$

□

Corollary 1.2.21. *Let R be a ring. Then for any $n > 0$, we have an equivalence of categories R-$\underline{\mathrm{mod}} \cong \mathrm{M}\text{-}\underline{\mathrm{mod}}_n(R)$.*

Proof. This follows from Theorem 1.2.20 via the right R-progenerator $P = R^n$. □

[1]The R-module structure on $\mathrm{Hom}_S(P,N)$ is defined as follows. For $f \in \mathrm{Hom}_S(P,N)$, set $af(p) = f(pa)$. We then check that $(a(bf))(p) = (bf)(pa) = f(pab)$.

1.3 Linear algebra over division rings

Lemma 1.3.1. *Let D be a division ring. Then every D-module is free.*

Unlike in the case of a commutative field, one now has the need to distinguish between right and left vector spaces, and, perhaps surprisingly, these categories may well be non-equivalent.

From some perspective it is natural to consider right D-vector spaces, as these have their linear transformations acting on the left, having the effect of making commutativity of the action be interpretable as a kind of associativity (see the discussion at the beginning of Section 1.1.1). In particular, we see that

$$\mathrm{Hom}_{\text{right } D\text{-mod}}(D, D) = D$$

where elements of D, viewed as endomorphisms, act as left multiplication. Consequently, from the usual identification

$$\mathrm{Hom}_R(M_1 \oplus M_2 \oplus \cdots \oplus M_m, N_1 \oplus N_2 \oplus \cdots \oplus N_n) = \begin{bmatrix} \mathrm{Hom}_R(M_1, N_1) & \mathrm{Hom}_R(M_2, N_1) & \cdots & \mathrm{Hom}_R(M_m, N_1) \\ \mathrm{Hom}_R(M_1, N_2) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \mathrm{Hom}_R(M_1, N_n) & \cdots & \cdots & \mathrm{Hom}_R(M_m, N_n) \end{bmatrix}$$

we find $\mathrm{End}_{\text{right } D\text{-mod}}(D^n) = \mathrm{M}_n(D)$ acting on column vectors on the left.

Exercise 1.3.2. *Show that there is a bijection between right ideals of $\mathrm{M}_n(D)$ and submodules of the right D-space D^n given by*

$$\left[I \lhd_r \mathrm{M}_n(D)\right] \mapsto \mathrm{Hom}(D^n, W) = \{\phi : D^n \to D^n \mid \mathrm{im}(\phi) \subset W\},$$

and a bijection between left ideals of $\mathrm{M}_n(D)$ and submodules of D^n given by

$$\left[I \lhd_\ell \mathrm{M}_n(D)\right] \mapsto \mathrm{Hom}(D^n/U, D^n) = \{\phi : D^n \to D^n \mid \ker(\phi) \supset U\}.$$

Exercise 1.3.3. *Show that we obtain from Exercise 1.3.2 a bijective correspondence*

$$\{\textit{rank } m \textit{ right ideals of } \mathrm{M}_n(D)\} \leftrightarrow \{\textit{rank } n - m \textit{ left ideals of } \mathrm{M}_n(D)\},$$

given by taking a right ideal $I \subset \mathrm{M}_n(D)$ to its left annihilator $J = \mathrm{ann}_{\ell, \mathrm{M}_n(D)}(I) = \{x \in \mathrm{M}_n(D) \mid xJ = 0\}$, and similarly taking a left ideal to its right annihilator.

1.4 Central simple algebras over fields

Recall that a ring (or algebra) is called simple if it has no two-sided ideals. If A is an F-algebra, it is called F-central if $\mathrm{Z}(A) = F$ and $\dim_F(A) < \infty$.

Definition 1.4.1. A central simple algebra over F is an F-algebra A which is simple and F-central. We say that A is a central division algebra over F if in addition A is a division algebra.

1.4.1 Simple rings (with finiteness conditions)

Noncommutative simple rings can have very intricate and complicated structures. On the other hand, in the presence of finiteness conditions, including such things as being a finite dimensional algebra over a field, satisfying the Artinian condition, etcetera, we find significant structural constraints on such algebras. As we will primarily be focused on finite dimensional algebras over fields, we will generally find ourselves in this context.

Let's first make a few quick observations about simple rings. First, that they are algebras over fields:

Lemma 1.4.2. *Let R be a simple ring. Then its center $\mathrm{Z}(R)$ is a field.*

Proof. Let $x \in \mathrm{Z}(R)\backslash 0$. Since x is central, $xR = Rx = RxR$ is the ideal generated by x. By assumption, since R is simple and $x \neq 0$, it follows $Rx = xR = R$ and therefore we can find elements $y, z \in R$ such that $yx = xz = 1$. Consequently, x is invertible in R. But now x central implies x^{-1} is as well, since $ax = xa$ implies $x^{-1}a = ax^{-1}$. Therefore $\mathrm{Z}(R)$ is a field. □

Consequently, when talking about simple rings, it always makes sense to consider them as algebras over some field F (which we can take, if we'd like, to be the center).

Next, we note the following well known result, which can be viewed as responsible for the ubiquity of division algebras in the study of more general rings and algebras.

Lemma 1.4.3 (Schur's Lemma)**.** *Let R be a k-algebra and M a simple left R-module. Let $D = \mathrm{End}_R(M)$. Then D is a division algebra over k.*

Proof. Let $d \in \mathrm{End}_R(M)$. Then as $\ker(d), \mathrm{im}(d)$ are submodules fo the simple module M, it follows that they are either 0 or M. If $\ker(d) = M$ or if $\mathrm{im}(d) = 0$ then d would be the 0 endomorphism. On the other hand, if these don't occur, then $\ker(d) = 0$ and $\mathrm{im}(d) = M$, which says d is a bijective endomorphism. One can now check that the inverse of an invertible endomorphism is itself an endomorphism, showing that $d^{-1} \in \mathrm{End}_R(M)$ whenever $d \neq 0$. Hence D is a division algebra. □

We will now aim to prove the following classification result, which can be viewed as a version of Wedderburn's structure theorem.

Theorem 1.4.4. *Let R be a simple ring containing a minimal left ideal. Then $R \cong \mathrm{M}_n(D)$ for some division ring D.*

In order to prove this, we will make use of the following result of Rieffel as described in [**?**, Lemma 2.1.6].

Lemma 1.4.5 (Rieffel)**.** *Suppose A is a simple F-algebra for some field F and $L \subset A$ is a minimal left ideal. Set $E = \mathrm{End}_F(L)$ and $B = \mathrm{End}_A(L) = \mathrm{C}_E(A)$. Then the natural map $A \to \mathrm{C}_E(B)$ is an isomorphism.*

In other words, in the language of Definition 1.2.11, L is faithfully balanced. Let's go ahead and see how this gives us our result:

Proof of Theorem 1.4.4. Let A be a simple F-algebra and let L be a minimal left ideal. Let $D = \mathrm{End}_A(L)$. By Lemma 1.4.3, D is a division algebra and by Lemma 1.4.5, $A \cong \mathrm{End}_D(L)$. Consequently A can be thought of as D-linear endomorphisms of the D-module L, which, by Lemma 1.3.1 has some free basis. We claim that L is finite dimensional over D, and hence $A \cong \mathrm{End}_D(D^n) = \mathrm{M}_n(D^{\mathrm{op}})$ for some D.

To show that L is finite dimensional over D, let us consider[2]

$$\mathscr{F} = \{\phi \in \mathrm{End}_D(L) = A \mid \text{ such that } \mathrm{im}\,\phi \text{ is finite dimensional}\}.$$

We claim that $\mathscr{F} = A$, which would tell us that $L = \mathrm{im}(\mathrm{id})$ is finite dimensional as claimed. In fact, it is easy to see that $\mathscr{F} \neq 0$ as it is possible to project onto a single basis vector via some (possibly infinite) basis for L. But we also claim that $\mathscr{F}$ is an ideal of $\mathrm{End}_D(L) = A$. This is because if $\phi \in \mathrm{End}_D(L)$, and $f \in \mathscr{F}$ then $\mathrm{im}\, f\phi \subset \mathrm{im}\, f$ and so $f\phi \in \mathscr{F}$. But $\mathrm{im}(\phi f) \subset \phi(\mathrm{im}\, f)$ so $\mathrm{im}\, f$ finite dimensional implies $\phi(\mathrm{im}(f))$ is as well, so $\phi f \in \mathscr{F}$. But since $A = \mathrm{End}_D(L)$ is simple, this implies $\mathscr{F} = A$ and so L is finite dimensional as claimed. □

It remains to prove the Lemma.

Proof of Lemma 1.4.5. Consider the map $\lambda : A \to E$ induced by left multiplication $a \mapsto (x \mapsto ax)$. By definition, $\lambda(A) \subset \mathrm{C}_E(B) = \mathrm{End}_B(L)$.

Our strategy will be to show that that $\lambda(L)$ is a left ideal of $\mathrm{C}_E(B) = \mathrm{End}_B(L)$. From this it would follow that $\mathrm{End}_B(L)\lambda(L) = \lambda(L)$. But since A is simple, $A = LA$ and so we would have

$$\begin{aligned}\lambda(A) = \lambda(LA) = \lambda(L)\lambda(A) = \mathrm{End}_B(L)\lambda(L)\lambda(A) = \mathrm{End}_B(L)\lambda(LA) \\ = \mathrm{End}_B(L)\lambda(A) \supset \mathrm{End}_B(L),\end{aligned}$$

which would give the reverse inclusion and complete the proof.

Let us then check that $\lambda(L)$ is a left ideal of $\mathrm{End}_B(L)$. For this, we need to see that if $\phi \in \mathrm{End}_B(L)$ and $x \in L$ then $\phi\lambda(x) \in \lambda(L)$. But if we let $y \in L$, then

$$(\phi\lambda(x))(y) = \phi(\lambda(x)y) = \phi(xy) = \phi(R_y(x))$$

where $R_y : L \to L$ is given by right multiplication by y. But we can see that R_y is an element of E which commutes with the action of A on the left and hence $R_y \in B$. But as ϕ is B-linear, it follows that

$$(\phi\lambda(x))(y) = \phi(R_y(x)) = R_y\phi(x) = \phi(x)y = \lambda(\phi(x)).$$

But as this is true for each y, we find $\phi\lambda(x) = \lambda(\phi(x)) \in \lambda(L)$ and so $\mathrm{End}_B(L)\lambda(L) \subset \lambda(L)$ as claimed. □

[2]Thanks to Yam Felsenstein for sharing this argument from his notes from a course by Eli Aljadeff.

Lemma 1.4.6. *Suppose A is a simple F-algebra admitting a minimal left ideal L. Then, every simple left A-module is isomorphic to L. Further, every left A-module is semisimple and can be written as a direct sum of copies of L.*

Proof. By Theorem 1.4.4 $A \cong \mathrm{M}_n(D) = \mathrm{End}_{\text{right-}D}(D^n)$, where $D = \mathrm{End}_A(L)$ is a division algebra. By Theorem 1.2.20 it follows that A-$\underline{\text{mod}} \cong D$-$\underline{\text{mod}}$. But as every left D-module is isomorphic to a direct sum of copies of D, and as D is the unique simple D-module, our equivalence of categories, described in Theorem 1.2.20 takes D to the simple module $L \cong D^n$. The result therefore follows from our equivalence of categories. □

Lemma 1.4.7. *Let F be a field and A a central simple F-algebra. Then $A \cong \mathrm{M}_n(D)$ for some F-central division algebra D. Furthermore, n is uniquely determined and D is unique up to isomorphism.*

Proof. By Theorem 1.4.4, we have $A \cong \mathrm{M}_n(D)$ for some division algebra D. It remains to show that D is also F-central and that D is unique up to unique isomorphism.

By Lemma 1.2.14, $F = \mathrm{Z}(A) = \mathrm{Z}(\mathrm{M}_n(D)) = \mathrm{C}_{\mathrm{M}_n(D)}(\mathrm{M}_n(D)) = \mathrm{C}_D(D) = \mathrm{Z}(D)$, and so D is also F-central (note it is evidently finite dimensional as it is a subspace of A).

On the other hand, if $\mathrm{M}_n(D) \cong \mathrm{M}_m(D')$ for some other division algebra D' then via Corollary 1.2.21, we have and equivalence of categories D-$\underline{\text{mod}} \cong D'$-$\underline{\text{mod}}$. But by Theorem 1.2.16, it follows that there is some right D-progenerator P and an isomorphism $D' \cong \mathrm{End}_{\text{right-}D}(P)$. But by Lemma 1.3.1, $P \cong D^m$ for some m and so $D' \cong \mathrm{M}_m(D)$. But since D' is division, this immediately implies $m = 1$ and so $D' \cong D$.

It remains to show that if $\mathrm{M}_n(D) \cong \mathrm{M}_m(D)$ then $n = m$. But this follows from the fact that the dimension (rank) of a D-vector space is well-defined. So $D^{n^2} \cong D^{m^2}$ implies $n = m$. □

Lemma 1.4.8. *Let A and B be F-algebras, and suppose that $A \otimes_F B$ is simple. Then A and B are both simple.*

Proof. This follows from the fact that if $I \lhd A$ is a proper ideal, then $I \otimes_F B \lhd A \otimes_F B$ is also a proper ideal (and similarly for ideals of B). □

For an F-algebra A, let $A^e = A \otimes_F A^{\mathrm{op}}$. This is often called the enveloping algebra of A. We have a natural map

$$\begin{aligned} A^e &\longrightarrow \mathrm{End}_F(A) \\ a \otimes b &\longmapsto (x \mapsto axb), \end{aligned}$$

which is sometimes referred to as the "sandwich map."

Lemma 1.4.9. *Let A be an F-algebra. Then with respect to the inclusion $\mathrm{End}_{A^e}(A) \subset \mathrm{End}_{\text{right-}A}(A) = A$, we have and identification $\mathrm{End}_{A^e}(A) = \mathrm{Z}(A)$.*

Proof. Suppose $x \in A$, and regard x as the element L_x of $\mathrm{End}_{\text{right-}A}(A)$ via $L_x(y) = xy$. Then $x \in \mathrm{Z}(A)$ if an only if $xy = yx$ for all y. Although somewhat redundant, this is equivalent to saying $xyzw = yxzw$ for all y, z, w. But

$$L_x(y \otimes z)(w) = L_x(ywz) = xywz \quad \text{and} \quad (y \otimes z)L_x(w) = (y \otimes z)(xw) = yxwz.$$

So we see that x is central in A if and only if $L_x(y \otimes z) = (y \otimes z)L_x$ for all y, z, which is to say, if and only if $L_x \in \mathrm{End}_{A^e}(A)$. □

1.4.2 Splitting central simple algebras

1.4.3 Characterizing central simple algebras

Lemma 1.4.10. *Let A be an F-algebra. Then A is a central simple F-algebra if and only if the sandwich map $A^e \to \mathrm{End}_F(A)$ is an isomorphism.*

Proof. We first note that if this is an isomorphism, then necessarily $\dim_F(A) < \infty$. Arguing by contradiction, suppose that A has a basis e_i, $i \in I$, with I infinite. Then $A \otimes_F A^{\mathrm{op}}$ has a basis of the form $e_i \otimes e_j$ indexed by $I \times I$, showing that the dimension of A^e is the same as that of A. On the other hand,

$$\mathrm{End}_F(A) = \mathrm{Hom}_F(\bigoplus_{i \in I} F, \bigoplus_{i \in I}, F) = \prod_{i \in I} \mathrm{Hom}_F(F, \bigoplus_{j \in I} F) = \prod_{i \in I} \bigoplus_{j \in I} F.$$

And the dimension of this space is at least as big as the dimension of $\prod_{i \in I} F$. But this space has dimension 2^I, yielding our contradiction.

Assuming that we have an isomorphism, it follows that $\mathrm{End}_F(A) \cong \mathrm{M}_{\dim_F(A)}(F)$ is simple, and therefore by Lemma 1.4.8, A is simple. But $\mathrm{Z}(A) = \mathrm{Z}(A) \otimes_F F \hookrightarrow \mathrm{Z}(A^e) = F$ tells us that $\mathrm{Z}(A) = F$ and so A is F-central.

For the converse, suppose A is a central simple algebra over F. As A^e-submodules of A are the same as ideals of A and A is simple, it follows that A is a simple module over A^e (via the standard "sandwich action" of A^e). But therefore, since A^e is a simple and finite dimensional F-algebra, it admits a minimal left ideal L (as one can choose one of minimal dimension), and by Lemma 1.4.6 any simple module is isomorphic to this one. That is, $L \cong A$ is left A^e-modules. But this implies that the map $A^e \to \mathrm{End}_{\mathrm{End}_{A^e}(A)}(A)$ is an isomorphism by Lemma 1.4.5. By Lemma 1.4.9, we can identify $\mathrm{End}_{A^e}(A) = \mathrm{Z}(A) = F$, which then gives us our desired isomorphism $A^e \to \mathrm{End}_F(A)$. □

It will be useful to have some tools to help understand the behavior of simplicity and centrality under tensor product. Let us start with an observation about the tensor product of associative algebras:

Exercise 1.4.11. *Let A, B, C be R-algebras for some commutative ring R. Then we have a natural identification*

$$\mathrm{Hom}_R(B \otimes_R C, A) = \left\{ (\phi_B, \phi_C) \in \mathrm{Hom}_R(B, A) \times \mathrm{Hom}_R(C, A) \;\middle|\; \begin{array}{c} \phi_B(B) \text{ and } \phi_C(C) \\ \text{commute in } A \end{array} \right\}.$$

Lemma 1.4.12. *Let B, C be algebras over F. If $B \otimes_F C$ is simple then B and C are both simple.*

Proof. We assume by contradiction that B is not simple. Let $I \lhd B$ be a proper ideal. Then it is straightforward to check that $I \otimes C$ is an ideal in $B \otimes C$, and by dimension count, it is also a proper ideal. □

We have a partial converse to this as well:

Lemma 1.4.13. *Let B be a central simple F algebra and let C be a simple F algebra. Then $B \otimes_F C$ is also simple.*

Proof. The strategy is as follows. As every two sided ideal is a kernel of a homomorphism, to show that an algebra is simple is the same as showing every (always unital) homomorphism must be injective. So, let us suppose we have a homomorphism $\phi : B \otimes C \to A$. As both B and C are simple, it follows that the restriction of ϕ to B and C gives injective homomorphisms. The result will now follow from the next lemma. □

Lemma 1.4.14. *Let B be a central simple F algebra and C a simple F-algebra. If $\phi_B : B \to A$ and $\phi_C : C \to A$ are (necessarily injective) homomorphisms such that $\phi_B(B)$ and $\phi_C(C)$ commute in A then the induced map $\phi : B \otimes C \to A$ is injective.*

Proof. As the maps ϕ_B and ϕ_C are injective, we may as well assume that B and C are subalgebras of A and that $C \subset \mathrm{C}_A(B)$. Now, as B is finite dimensional, any element of $B \otimes C$ can be written in the form $\alpha = \sum b_i \otimes c_i$ where the elements $b_i \in B$ are taken to be from an F-basis $\{b_1, \ldots, b_n\}$ of B. Futher, we have in this case $\alpha = 0$ if and only if $c_i = 0$ for all i. Therefore our goal is to show that $\sum b_i c_i = 0$ if and only if $c_i = 0$ for all i.

We note that A is a B^e-module as well as a right[3] C module, and as C commutes with B, the action of B^e and C on A commute with each other as well. Noting the isomorphism $B^e \to \mathrm{End}_F(B)$ via the sandwich map from **??**, we may in particular find, for each j, an element $T_j \in B^e$ such that $Tb_i = \delta_{i,j} 1_B = \delta_{i,j} 1_A$. We then find that:

$$\sum b_i c_i = 0 \implies T_j \sum b_i c_i = 0 \implies \sum (T_j b_i) c_i = 0 \implies c_j = 0,$$

for all j, as desired. □

We note, in particular we find:

Lemma 1.4.15. *Suppose B, C are finite dimensional F-subalgebras of an algebra A, with B central simple, C simple and $C \subset \mathrm{C}_A(B)$. Then the following are equivalent:*

1. $A = BC$,
2. $A \cong B \otimes C$,
3. $(\dim A) = (\dim B)(\dim C)$.

[3] although both sides work fine!

Let us now record an observation about tensor products of vector spaces:

Lemma 1.4.16. *Suppose we have F-vector spaces and subspaces $W_1 < V_1$, $W_2 < V_2$. Then as a subspace of $V_1 \otimes V_2$ we have*

$$(W_2 \otimes V_1) \cap (W_1 \otimes V_2) = W_1 \otimes W_2.$$

Proof. Exercise. □

This gives a useful characterization of centers of tensor products:

Lemma 1.4.17. *Let B, C be F-algebras. Then $Z(B \otimes C) = Z(B) \otimes Z(C)$.*

Proof. It is clear that $Z(B) \otimes Z(C) \subset Z(B \otimes C)$. For the converse, we note that $Z(B \otimes C) \subset$
$C_{B \otimes C}(F \otimes C) = B \otimes Z(C)$, and similarly $Z(B \otimes C) \subset Z(B) \otimes C$. Consequently we have by **??**, $Z(B \otimes C) \subset (B \otimes Z(C)) \cap (Z(B) \otimes C) = Z(B) \otimes Z(C)$, completing the proof. □

These can be put together in the following useful observation:

Proposition 1.4.18. *Suppose A is a central simple F-algebra and E/F is a field extension. Then $A \otimes_F E$ is a central simple E-algebra.*

Proof. By **??**, we see that $A \otimes_F E$ is a simple algebra, which is clearly finite dimensional over E. By **??**, we see $Z(A \otimes_F E) = Z(A) \otimes_F Z(E) = E$. □

We now come to our main result characterizing central simple algebras:

Proposition 1.4.19. *Let A an algebra over a field F. Then the following conditions are equivalent:*

1. *A is a central simple F-algebra,*
2. *$A \cong \mathrm{M}_n(D)$ where D is an F-central division algebra,*
3. *The "sandwich map" $A \otimes_F A^{\mathrm{op}} \to End_F(A)$ via $a \otimes b \mapsto (x \mapsto axb)$ is an isomorphism,*
4. *there exists an F-algebra B such that $A \otimes B \cong \mathrm{M}_n(F)$ for some n,*
5. *there exists an F-algebra B such that $A \otimes B$ is a central simple F-algebra,*
6. *there exists a field extension E/F such that $A \otimes E \cong \mathrm{M}_n(E)$ for some n,*
7. *there exists a separable field extension E/F such that $A \otimes E \cong \mathrm{M}_n(E)$ for some n,*
8. *$A \otimes \overline{F} \cong \mathrm{M}_n(\overline{F})$ for some n,*
9. *A be a projective module over the enveloping algebra $A \otimes_F A^{\mathrm{op}}$.*

One more equivalent condition we didn't prove, but which is worth mentioning is that A be a projective module over the enveloping algebra $A \otimes_F A^{\mathrm{op}}$ (i.e. the multiplication map $A \otimes A^{\mathrm{op}} \to A$ splits).

1.5 Azumaya algebras over commutative rings

To generalize from fields to commutative rings, we define the concept of Azumaya.

In the following proposition, for a commutative ring R and a prime $\mathfrak{p} \in \mathrm{Spec}(R)$, we will write $\kappa(\mathfrak{p})$ to denote the field $\mathrm{frac}(R/\mathfrak{p})$ (also called the residue field of $\mathfrak{p}$).

Proposition 1.5.1. *For an algebra A over a commutative ring R which is finitely generated and projective as a module, the following are equivalent:*

1. *for every $\mathfrak{p} \in \mathrm{Spec}(R)$, $A \otimes_R \kappa(\mathfrak{p})$ is a central simple $\kappa(\mathfrak{p})$-algebra,*
2. *the sandwich map $A \otimes_R A^{\mathrm{op}} \to End_R(A)$ is an isomorphism.*

Definition 1.5.2. If the equivalent conditions of Proposition 1.5.1 hold, we say that A is an Azumaya algebra over R (also called a central separable algebra over R).

In order to prove this proposition, we will require a slight detour into some commutative algebra.

1.5.1 Commutative algebra detour

Recall for a commutative ring R, we write $\mathrm{Spec}\, R$ to denote the collection of prime ideals of R. For $f \in R$, we write R_f for the localization $R[f^{-1}]$ and for $\mathfrak{p} \in \mathrm{Spec}\, R$, we write $R_{\mathfrak{p}}$ for the localization $R[(R \backslash \mathfrak{p})^{-1}]$. In particular, $R_{\mathfrak{p}} = \varinjlim R_f$ is the colimit of the rings R_f taken over all $f \notin \mathfrak{p}$. We set $D_f = \{\mathfrak{p} \in \mathrm{Spec}\, R \mid f \notin \mathfrak{p}\}$ and note that we have a bijection $D_f \cong \mathrm{Spec}\, R_f$ via $\mathfrak{p} \mapsto \mathfrak{p}R_f$.

Definition/Lemma 1.5.3. *For a commutative ring R, the sets D_f form a basis for a topology, and we define the Zariski topology on* $\mathrm{Spec}\, R$ *to be the topology generated by the sets D_f.*

For a commutative ring R and a prime $\mathfrak{p} \in \mathrm{Spec}\, R$, we write $R_{\mathfrak{p}}$ to denote the localization of R at $\mathfrak{p}$.

Definition 1.5.4. Let R be a commutative ring.

Just as a side comment – it turns out that when A/R is Azumaya it will follow that A is finitely presented as an R module and is a generator in the category of R modules (recall that M is a generator if for every other R-module N, there is a surjective map $M^{\oplus I} \twoheadrightarrow N$ for some index set I). So being an Azumaya algebra imposes serious module-theoretic constraints on an algebra.

1.6 Galois extension of rings

Much like the story for division algebras, while we may start by wanting to construct interesting examples of (central) division algebras, it is useful to consider instead central simple algebras. There are a few natural reasons that this kind of consideration comes up:

- many natural constructions which sometimes yield division algebras will often produce central simple algebras instead,
- when we construct central simple algebras, by the Wedderburn structure theorem, we may find that we have constructed division algebras within them,
- division algebras are not "preserved by scalar extension." In other words, if D/F is a central division algebra, and E/F is a field extension, $D \otimes_F E$ will be central simple, but need not be division.

A very similar discussion arises when considering Galois extension, which leads us to consider the concept of Galois extensions of the form E/F where E need not be a field. From here we will then proceed to consider the case where both F and E are replaced by more general commutative rings (in some analogy with the concept of Azumaya algebras).

1.6.1 Etale extensions of fields

Let's start with the generalization of the concept of a (not necessarily Galois) separable field extension, before considering the Galois case:

Definition 1.6.1 (Etale extensions of fields)**.** Let F be a field. We say that a commutative F-algebra E/F is étale over F if we can write E as a finite (possibly empty) product $E = \bigtimes_{i \in I} E_i$ where each E_i is a separable field extension of F.

We note that in the literature, one also says that E/F is a separable extension of rings.

A strange digression into empty rings

Let us take just a moment to discuss the edge case in which the product is empty. By convention, an empty product is a final object in a category, and here, considering ourselves to be in the category of unital commutative rings, we find that this final object is the "zero ring," consisting of a single element $0 = 1$. While this ring is not actually a field (because, for example, its nonzero elements fail to form a group, not having an identity element), we still consider the zero ring to be a product of fields, as it is an empty product of fields. Consequently it is an étale extension of every field.

1.6.2 Galois étale extensions of fields

We may or may not get to proving all these equivalent conditions, but here are some ways we can characterize what it means for an étale extension to be Galois.

Recall the following definition:

Definition 1.6.2. Let S be a ring and G a finite group acting on S as automorphisms. We define $(S, G, 1)$, the twisted group ring, to be the algebra generated by S and symbols u_σ for $\sigma \in G$, so that as a left S-module we have

$$(S, G, 1) = \bigoplus_{\sigma \in G} S u_\sigma,$$

with multiplication given by the rules

$$u_\sigma u_\tau = u_{\sigma\tau} \quad \text{and} \quad u_\sigma x = \sigma(x) u_\sigma, \text{ for } x \in S, \sigma, \tau \in G.$$

Definition/Lemma 1.6.3. *Let F be a field and E a commutative F-algebra and let $G \subseteq \mathrm{Aut}(E/F)$ be a group of automorphisms of E fixing F. We say that E is a G-Galois extension of F if the following equivalent conditions hold:*

1. *$|G| = \dim_F E$ and $E^G = F$,*
2. *$(E, G, 1)$ is a central simple F-algebra,*
3. *the natural map $(E, G, 1) \to \mathrm{End}_F(E)$ is an isomorphism,*
4. *the natural map $(E, G, 1) \to \mathrm{End}_F(E)$ is injective (i.e. Dedekind's Lemma holds),*
5. *we can write $E = \bigotimes_{i \in I} E_i$ with E_i/F separable extensions, and such that the induced action of G on I is transitive and for each $i \in I$, E_i/F is $Stab_G(i)$-Galois.*

An important thing to note is that there is generally no canonical choice for the group G for a given F-algebra E. So, for example, the $\mathbb{R}$-algebra $\mathbb{C} \times \mathbb{C}$ can be regarded as Galois

- with respect to the group $C_2 \times C_2 = \langle \sigma, \tau \mid \sigma^2, \tau^2 \rangle$ via the action $\sigma(z_1, z_2) = (z_2, z_1)$ and $\tau(z_1, z_2) = (\overline{z}_1, \overline{z}_2)$, or
- with respect to the group $C_4 = \langle \gamma \mid \gamma^4 \rangle$ via the action $\gamma(z_1, z_2) = (z_2, \overline{z}_1)$.

1.6.3 Etale extensions of commutative rings

We will come back to this a bit later when considering étale cohomology and more general descent, but let's define, as we are now able to, the notions of what it means for an extension of commutative rings to be étale.

Definition 1.6.4. Let R be a commutative ring. We say that an R-algebra S is étale if it is finitely ***presented*** ~~generated~~ and flat as an R-module, and if, for every $\mathfrak{p} \in \mathrm{Spec}(R)$, we have $S \otimes_R \kappa(\mathfrak{p})$ is an étale extension of the field $\kappa(\mathfrak{p})$.

1.6.4 Galois extensions of commutative rings

As with the notion of Azumaya, we are now ready to present the notion of what it means for an extension of rings to be Galois.

Definition/Lemma 1.6.5. *Let R be a commutative ring and S a commutative R-algebra. Let $G \subseteq \mathrm{Aut}(S/R)$ be a group of automorphisms of S fixing R. We say that S is a G-Galois extension of R if the following equivalent conditions hold:*

1. *for every $\mathfrak{p} \in \mathrm{Spec}(R)$, $S \otimes_R \kappa(\mathfrak{p})$ is a G-Galois extension over $\kappa(\mathfrak{p})$,*
2. *$(S, G, 1)$ is an Azumaya algebra over R,*
3. *the natural map $(S, G, 1) \to \mathrm{End}_R(S)$ is an isomorphism.*

While not obvious from the definitions, the condition that S/R is G-Galois also imposes strong module-theoretic constraints on S, namely that S is a finitely generated projective R-module which is a generator in the category of R-modules. These conditions also imply that $S^G = R$ (as expected from usual Galois theory).

1.7 Galois Descent – an equivalence of categories

One important consequence of Definition/Lemma 1.6.5 this is that the Morita theorems apply (see Proposition A.1.2), and we obtain an equivalence of categories as follows:

Lemma 1.7.1. *Let S/R be a G-Galois extension of commutative rings. Then we obtain an equivalence of categories*

$$R\text{-modules} \leftrightarrow (S, G, 1)\text{-modules}$$
$$M \mapsto S \otimes_R M$$

via the standard $(S, G, 1) \cong \mathrm{End}_R(S)$-module structure on S.

We can make this particularly useful by recalling the notion of semilinear actions.

Definition 1.7.2. Let G be a group acting on a commutative ring S and let M be an S-module. A G-semilinear action on M is an action of G on M as an Abelian group such that for each $\sigma \in G$, $m \in M$, $x \in S$, we have $\sigma(xm) = \sigma(x)\sigma(m)$.

A G-semilinear S-module is defined to be an S-module with a G-semilinear action.

We may then consider the category of such G-semilinear S-modules and observe that this category is also equipt with a tensor product (monoidal) structure. That is, if $\mathrm{M}_1, \mathrm{M}_2$ are G-semilinear S-modules, we can define $\mathrm{M}_1 \otimes_S \mathrm{M}_2$ to have a G-semilinear action via

$$\sigma(m_1 \otimes m_2) = \sigma(m_1) \otimes \sigma(m_2).$$

With this notion, we can then define the notion of a G-semilinear S-algebra (via its structural maps such as $A \otimes_S A \to A$ satisfying various axioms).

We note the following fact, which is easily verified via the definitions:

Lemma 1.7.3. *Let S be a ring with an action of a group G. Then there is an equivalence (actually an isomorphism) of categories between $(S, G, 1)$-modules G-semilinear S-modules.*

Combining Lemma 1.7.3 with Lemma 1.7.1, we obtain the following:

Theorem 1.7.4 (Galois descent)**.** *Let S/R be a G-Galois extension of commutative rings. Then we obtain an equivalence of categories*

$$\begin{aligned} R\text{-modules} &\leftrightarrow G\text{-semilinear } S\text{-modules} \\ M &\mapsto S \otimes_R M \\ N^G &\leftarrow\!\shortmid N. \end{aligned}$$

Furthermore, this equivalence respects tensor products.

We verified implicitly that one of these directions gives an equivalence (at least, by quoting Morita theory). The other direction is given in the exercises.

1.8 Galois Descent – twisted forms and obstructions

The fundamental question of Galois descent is the following: given a G-Galois extension of commutative rings S/R, how can one go between algebraic structures over R and algebraic structures over S? We can phrase this in terms of two concrete questions:

Question 1.8.1. *Given an R algebra A, how can we describe all R algebras A' such that $A \otimes S \cong A' \otimes S$?*

Question 1.8.2. *Given an S algebra B, when can we find an R algebra A such that $A \otimes S \cong B$?*

Twisted forms and H^1

Question 1.8.1 is in large part the subject of the exercises, and we recall here the conclusions. In the context of Theorem 1.7.4, we can reframe this first question as follows. Given a semilinear action of G on an S-algebra B (for example, $B = S \otimes A$), how can we describe all other semilinear actions on B. These other actions, via Theorem 1.7.4, would correspond to R-algebras A' such that $S \otimes A' \cong B$. Recall the following definitions:

Definition 1.8.3. Let X, Y be sets with action by a group G. Then we obtain a natural action on the set of maps $Map(X, Y)$ via $(\sigma \cdot f)(x) \equiv \sigma(f(\sigma^{-1}(x)))$.

Definition 1.8.4. Let G, A be groups, and suppose we have a homomorphism $G \to \mathrm{Aut}(A)$ providing an action of G on A. We say that a map $\alpha : G \to A$ is a crossed homomorphism, or a 1-cocycle, if

$$\alpha(\sigma\tau) = \alpha(\sigma)\sigma(\alpha(\tau)), \quad \forall \sigma, \tau \in G.$$

We write $Z^1(G, A)$ for the set of all crossed homomorphisms.

Definition 1.8.5. The group A acts on $Z^1(G, A)$ via $(a \cdot \alpha)(\sigma) = a\alpha(\sigma)\sigma(a)^{-1}$, and we define $\mathrm{H}^1(G, A) = Z^1(G, A)/A$ to be the set of orbits under this action.

We note that in the case A is an Abelian group, this corresponds to the standard group cohomology construction, and the sets $Z^1(G, A)$ and $\mathrm{H}^1(G, A)$ have natural group structure given by pointwise multiplication in A. In general, however, these are just sets with distinguished elements (pointed sets), where the distinguished element comes from the crossed homomorphism $G \to A$ sending all elements to the identity.

Proposition 1.8.6. *Let B be a G-semilinear S-algebra, with action written as $(\sigma, b) \mapsto \sigma b$. Consider the G-action on $\mathrm{Aut}_S(B)$ given by Definition 1.8.3. Then if we have any other G-semilinear action on B, $(\sigma, b) \mapsto \sigma \cdot b$, then we may find a crossed homomorphism $\alpha : G \to \mathrm{Aut}_S(B)$ such that*

$$\sigma \cdot b = \alpha(\sigma)\sigma b,$$

and this gives a bijection between crossed homomorphism and semilinear actions.

Further, if $\alpha, \beta \in Z^1(G, \mathrm{Aut}_S(B))$ are crossed homomorphisms, then the resulting semilinear algebras are isomorphic if and only if α and β are in the same $\mathrm{Aut}_S(B)$ orbit. In particular, we have a bijection between isomorphism classes of algebras A'/R such that $S \otimes A' \cong B$ and the pointed set $\mathrm{H}^1(G, \mathrm{Aut}_S(B))$.

Descent obstructions and H^2

We now consider the Question 1.8.2 – given an S-algebra B, when can we find an R-algebra A such that $S \otimes_R A \cong B$? In light of Theorem 1.7.4, this is equivalent to asking the question of when we are able to define a semilinear action of G on B.

To make this easier to work with, let's define a bit of language:

Definition 1.8.7. Let B be an S-algebra and let σ be an automorphism of S. We define a new S-algebra, denoted ${}^{\sigma}S$ to have underlying set ${}^{\sigma}x$, $x \in S$ (that is, there is a bijection between the elements of B and ${}^{\sigma}B$), with operations:

$${}^{\sigma}x + {}^{\sigma}y = {}^{\sigma}(x + y), \qquad ({}^{\sigma}x)({}^{\sigma}y) = {}^{\sigma}(xy), \qquad \forall x, y \in B$$

and with S-module structure given by:

$$\lambda \, {}^{\sigma}x = {}^{\sigma}(\sigma^{-1}(\lambda)x), \qquad \forall \lambda \in S, x \in B,$$

or in other words, $\sigma(\lambda) \, {}^{\sigma}x = {}^{\sigma}(\lambda x)$.

Example 1.8.8. *As an example, note that if B is an S-algebra with a free S-module basis e_i and with multiplication table given by*

$$e_i e_j = \sum_k c_{i,j}^k e_k,$$

then the algebra ${}^\sigma B$ has multiplication table given by

$${}^\sigma e_i \, {}^\sigma e_j = \sum_k \sigma(c_{i,j}^k) \, {}^\sigma e_k.$$

Now, back to the case of a G-Galois extension S/R and an S-algebra B, we would like to ask whether or not it is possible to define a semilinear action of G on B. This amounts to defining, for every $\sigma \in G$ a "possible action,"

$$\phi_\sigma : B \to B$$

which will satisfy $\phi_\sigma(\lambda x) = \sigma(\lambda)\phi_\sigma(x)$ for $\lambda \in S, x \in B$, and such that $\phi_\sigma \phi_\tau = \phi_{\sigma\tau}$. One complicating factor is that such maps ϕ_σ are evidently not S-linear, but we can change our perspective by considering the corresponding maps $\psi_\sigma : {}^\sigma B \to B$ given by $\psi_\sigma({}^\sigma x) = \phi_\sigma(x)$. For this map, we find

$$\psi_\sigma(\lambda \, {}^\sigma x) = \psi_\sigma({}^\sigma(\sigma^{-1}(\lambda)x)) = \phi_\sigma(\sigma^{-1}(\lambda)x) = \lambda\phi_\sigma(x) = \lambda\psi_\sigma({}^\sigma x),$$

which allows us to encode the information of ϕ_σ as an S-linear map ψ_σ. If we let $\sigma : B \to {}^\sigma B$ denote the map $x \mapsto {}^\sigma x$ (which we can think of as a "universal" σ-linear map), then we can consider this via the following diagram

$$\begin{array}{ccc} {}^\sigma B & \xrightarrow{\psi_\sigma} & B \\ {\scriptstyle\sigma}\uparrow & & \| \\ B & \xrightarrow[\phi_\sigma]{} & B \end{array}$$

as $\psi_\sigma(x) = \sigma(\phi_\sigma(\sigma^{-1}x))$. More generally, we may "twist" these to obtain maps

$$\begin{array}{ccc} {}^{\sigma\tau} B & \xrightarrow{{}^\sigma\psi_\tau} & {}^\sigma B \\ {\scriptstyle\sigma}\uparrow & & \uparrow{\scriptstyle\sigma} \\ {}^\tau B & \xrightarrow[\psi_\tau]{} & B \end{array}$$

$$\begin{aligned} {}^\sigma\psi_\tau : {}^{\sigma\tau}B &\to {}^\sigma B, \\ {}^{\sigma\tau}x &\mapsto {}^\sigma(\psi_\tau({}^\tau x)) = {}^\sigma\phi_\tau(x). \end{aligned}$$

This perspective allows us to interpret the condition $\phi_\sigma\phi_\tau = \phi_{\sigma\tau}$ in terms of S-linear maps. That is, we have

$$\begin{aligned} \psi_{\sigma\tau} : {}^{\sigma\tau}B &\to B, \\ {}^{\sigma\tau}x &\mapsto \phi_{\sigma\tau}(x), \end{aligned}$$

and,

$$\begin{aligned}\psi_\sigma{}^\sigma\psi_\tau : {}^{\sigma\tau}B &\to B,\\ {}^{\sigma\tau}x &\mapsto \phi_\sigma\phi_\tau(x).\end{aligned}$$

Consequently, the condition $\phi_\sigma\phi_\tau = \phi_{\sigma\tau}$ corresponds to the condition $\psi_{\sigma\tau} = \psi_\sigma{}^\sigma\psi_\tau$.

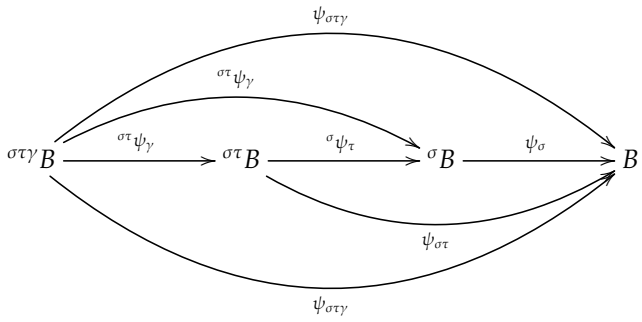
Analyzing the possibilities, we see:

Case 1: ${}^\sigma B$ and B are not isomorphic for some $\sigma \in G$.
In this case, there is no possible way that σ can act on B, and so no hope for defining a semilinear action of B. Consequently, there is no algebra A/R such that $S \otimes A \cong B$.

Case 2: There exist isomorphisms $\psi_\sigma : {}^\sigma B \xrightarrow{\sim} B$ for each $\sigma \in G$.
In this case, we need only consider whether or not these can be chosen so that $\psi_{\sigma\tau} = \psi_\sigma{}^\sigma\psi_\tau$. To measure our "distance" from this condition, and make a connection with group cohomology, we define:[4]

$$\beta(\sigma,\tau) = \psi_{\sigma\tau}^{-1}\psi_\sigma{}^\sigma\psi_\tau \in \mathrm{Aut}_S(B).$$

We are successful if we can choose ϕ_σ so as to make $\beta(\sigma,\tau) = 1$ for all σ,τ. Tracing the following diagram:



we find

$$\beta(\sigma\tau,\gamma)\beta(\sigma,\tau) = \beta(\sigma,\tau\gamma)\ \psi_\sigma{}^\sigma\beta(\tau,\gamma)\psi_\sigma^{-1}.$$

which we can think of as a nonabelian version of a 2-cocycle condition, although we won't try to define this "cohomology set" precisely here.

Of course, changing our isomorphisms ϕ_σ (and hence the maps ψ_σ) will alter our choice of β's. More precisely, if $\phi'_\sigma : B \to B$ is another σ-linear isomorphism, with corresponding isomorphism $\psi'_\sigma : {}^\sigma B \to B$, we see that $\psi'_\sigma\psi_\sigma^{-1} \equiv \rho(\sigma) \in \mathrm{Aut}_S(B)$, and so $\psi'_\sigma = \rho(\sigma)\psi_\sigma$ for some unique automorphism $\rho(\sigma)$, and conversely, different choices of isomorphisms ψ correspond to arbitrary functions $\rho : G \to \mathrm{Aut}_S(B)$. Given such a ρ corresponding to ϕ', we find that the corresponding β' is given by

$$\beta'(\sigma,\tau) = (\psi'_{\sigma\tau})^{-1}\psi'_\sigma{}^\sigma\psi'_\tau = \psi_{\sigma\tau}^{-1}\rho(\sigma\tau)^{-1}\rho(\sigma)\psi_\sigma\ {}^\sigma\rho(\tau)\ {}^\sigma\psi_\tau.$$

[4]note, this is a somewhat different convention than the one we did in class

In general, this is a difficult formula to interpret, but with sufficient commutativity, it will reduce to the standard notion of 2-cocycles and their equivalence via differing by a coboundary.

We note that the previous machinery, which was introduced in the context of ring extensions, works perfectly well for schemes as well. Let's gather these definitions and observations in this situation:

Definition 1.8.9. Let $X = (X, \mathcal{O}_X)$ be a scheme and let $\mathcal{A}$ be a quasicoherent sheaf of associative $\mathcal{O}_X$ algebras. We say that $\mathcal{A}$ is Azumaya if for every affine open set $\operatorname{Spec} R = U \subseteq X$, $\mathcal{A}(U)$ is an Azumaya algebra over R.

We see, essentially as a consequence of Proposition 1.5.1, that we can characterize Azumaya-ness as follows. Here for a scheme X and a point $x \in X$, we write $\kappa(x)$ for the residue field of x – that is, $\kappa(x) = \mathcal{O}_{X,x}/\mathfrak{m}_{X,x}$. If $\mathcal{F}$ is a sheaf of $\mathcal{O}_X$ algebras, we write $\mathcal{F}|_x$ to mean $\mathcal{F}_x \otimes_{\mathcal{O}_{X,x}} \kappa(x)$.

Proposition 1.8.10. *For a scheme X and $\mathcal{A}$ a locally free and finitely generated sheaf of associative $\mathcal{O}_X$ algebras, the following are equivalent:*

1. *$\mathcal{A}$ is Azumaya,*
2. *for every point $x \in X$, $\mathcal{A}|_x$ is a central simple algebra over $\kappa(x)$,*
3. *the sandwich map $\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{A}^{\mathrm{op}} \to \mathscr{E}\mathrm{nd}_{\mathcal{O}_X}(\mathcal{A})$ is an isomorphism (here $\mathscr{E}\mathrm{nd}$ denotes the endomorphism sheaf).*

Proof. We leave the verification of this as an exercise, via Proposition 1.5.1. □

Next, we define the notion of an étale morphism, relying on the corresponding definition for rings from Definition 1.6.4.

Definition 1.8.11. Let $f : X \to Y$ be a morphism of schemes. We say that f is étale at $x \in X$ if there exists an affine open neighborhood $\operatorname{Spec} B = V \subseteq X$ of x, and an affine open neighborhood $\operatorname{Spec} A = U \subseteq Y$ containing $f(U)$, such that B is an étale ring extension of A.

One thing that this definition should emphasize is that this definition is local on X[5]. The following definition connects more directly to Definition 1.6.4.

Lemma 1.8.12. *Let $f : X \to Y$ be a morphism of schemes. Then f is étale if and only if it is flat, locally of finite presentation, and for every $y \in Y$, the fiber $X_y = X \times_Y y$ is the spectrum of an étale (commutative ring) extension of the field $\kappa(y)$.*

Proof. [**?**, Tag 02GM] □

Let's now define the notion of a Galois extension of schemes. Note that, unlike the case of étale ring extensions, Galois extensions of rings are necessarily flat and locally free of finite rank. In particular, these are module finite maps. It

[5] as an illustrative example, the doubled affine line mapping to the affine line is, locally on the domain, an isomorphism and hence étale

follows that the corresponding type of map for schemes would be a finite map, and as such would be affine. Hence, we can talk about Galois extensions either as morphisms of schemes $f : X \to Y$, or as coherent sheaves of commutative $\mathcal{O}_Y$-algebras corresponding to $f_*\mathcal{O}_X$.

Definition/Lemma 1.8.13. *Let Y a scheme and $\mathcal{R}$ a sheaf of commutative $\mathcal{O}_Y$ algebras, which are locally free of finite type as $\mathcal{O}_Y$-modules. Suppose that G is a finite group of $\mathcal{O}_Y$-linear automorphisms of $\mathcal{R}$. We say that f is a G-Galois extension if the following equivalent conditions are true:*

1. *for every open affine $\operatorname{Spec} S \subseteq Y$, $\mathcal{R}(\operatorname{Spec} S)/S$ is G-Galois,*
2. *the sheaf of algebras $(\mathcal{R}, G, 1)$ is Azumaya over $\mathcal{O}_Y$,*
3. *the natural map $(\mathcal{R}, G, 1) \to \mathscr{E}\mathrm{nd}_{\mathcal{O}_Y}(\mathcal{R})$ is an isomorphism,*
4. *for every $y \in Y$, $\mathcal{R}|_y$ is a G-Galois commutative ring extension of the field $\kappa(y)$ (as in Definition/Lemma 1.6.5, **??**).*

The machinery of Section 1.8 goes through as previously described, and we will work through it via an example:

1.8.1 Galois descent for line bundles

need to fill in this section

Chapter 2

Geometry

2.1 Etale descent – an equivalence of categories

We would like to ask a question which is analogous to those we asked in Section 1.8, in the context of morphisms of schemes. Namely, for a morphism of schemes $\pi : X \to U$, how can one go between structures on U and structures on X. That is, we have a natural functor π^*, taking sheaves on U to sheaves on X. In some sense, this is a forgetful process. We would like to know how much information is lost, and what additional information is needed to "go backwards."

We will use the psychological crutch of considering the case that X is a disjoint union of schemes $X = \sqcup U_i$ so that the individual morphisms $\pi_i : U_i \to U$ are étale morphisms. But we will visualize these maps as open covers in terms of intuition. We will write $U_{i,j}$ for the fiber product $U_i \times_U U_j$, which we will think of as the analog of the intersection of two open sets. Similarly we define $U_{i,j,k}$ as the triple fiber product $U_i \times_U U_j \times_U U_k$, etcetera. We write $\pi_{i,j}$ to denote the map $U_i \times_U U_j \to U$ (via the equal morphisms induced by π_i or π_j).

In order to reduce the notational clutter, if $\mathscr{F}$ is a sheaf of $\mathcal{O}_U$-modules, we will write $\mathscr{F}|_{i,j}$ to denote the sheaf $\pi_{i,j}^* \mathscr{F}_{i,j}$, and similarly for triple fiber products, etc.

So as to eliminate all possible suspense, let us simply give the "answer:" We first recall the notion of an étale covering:

Definition 2.1.1. Let U be a scheme and $\mathscr{U} = \{\pi_i : U_i \to U\}$ a family of morphisms. We say that $\mathscr{U}$ is an étale covering of U if for all i, π_i is an étale morphism, and if the family is jointly surjective. That is, if for every $y \in U$ a scheme-theoretic point, there exists $u \in U_i$ for some i a scheme theoretic point, such that $\pi_i(u) = y$.

Definition 2.1.2. If $\mathscr{U} = \{\pi_i : U_i \to U\}$ is a family of morphisms, we define the descent category $\mathrm{Desc}(\mathscr{U}, \mathrm{QCoh})$ to be the category whose objects are pairs $((\mathcal{F}_i), (\phi_{i,j}))$ where each $\mathcal{F}_i$ is a quasicoherent sheaf over U_i and where $\phi_{i,j}$:

$\mathcal{F}_i|_{i,j} \to \mathcal{F}_j|_{i,j}$ are isomorphisms such that for all i, j, k, we have

$$\phi_{i,k}|_{i,j,k} = \phi_{j,k}|_{i,j,k} \circ \phi_{i,j}|_{i,j,k}.$$

Note that in the case where $\mathscr{U}$ is an open covering, this is just describing gluing data for sheaves (see [**?**, Exercise II.1.22]). We say that descent holds if sheaves are exactly described by such gluing data. Note that there is always a canonical functor $\mathrm{QCoh}_U \to \mathrm{Desc}(\mathscr{U}, \mathrm{QCoh})$ taking a sheaf $\mathcal{F}$ on U to the tuple $((\mathcal{F}|_i), (1_{i,j}))$, where $1_{i,j}$ represents the canonical identification of $\mathcal{F}|_i|_{i,j}$ with $\mathcal{F}|_j|_{i,j}$ (both being canonical equal to $\mathcal{F}|_{i,j}$).

Theorem 2.1.3 (Etale descent)**.** *Let $\{\pi_i : U_i \to U\}$ be an étale covering. Then the natural functor $\mathrm{QCoh}_U \to \mathrm{Desc}(\mathscr{U}, \mathrm{QCoh})$ given by $\mathcal{F} \mapsto ((\mathcal{F}|_i), (1_{i,j}))$ is an equivalence of categories.*

Proof. See (for a somewhat more general context) [**?**, Tag 023T]. □

2.2 Sites, sheaves and stacks

In fact, and possibly we should have started here, descent is closely tied to the notion of a sheaf itself in the context of a Grothendieck topology.

Definition 2.2.1 (Grothendieck topologies and sites)**.** Let C be a category. A Grothendieck topology τ on C is a set whose elements are collections of morphisms with common codomain $\{U_i \to U\}_{i \in I}$, which we call covers, with the following properties:

1) if $\{U' \to U\}$ is a family consisting of a single isomorphism, then $\{U' \to U\} \in \tau$,

2) if $\{U_i \to U\} \in \tau$ and $V \to U$ is a morphism in C then the fiber products $U_i \times_U V$ exist and $\{U_i \times_U V \to V\} \in \tau$,

3) if $\{U_i \to U\} \in \tau$ and if $\{V_{i,j} \to U_i\} \in \tau$ for each i, then the family obtained by compositions $\{V_{i,j} \to U\}$ is also in τ.

We define a site to be a pair $C = (C, \tau_C)$ where C is a category and τ_C is a Grothendieck topology on C.

Example 2.2.2 (the site of a topological space)**.** *Let X be a topological space. The category $Op(X)$, whose objects are open subsets of X and whose morphisms are inclusions admits a Grothendieck topology by declaring that the open covers are families of inclusions $\{U_i \to U\}$ which are jointly surjective (i.e. which cover U).*

This is the main motivating example, and the notation which is often used for sites reflects this. The following definition is a typical case in point.

Example 2.2.3 (the big site of a topological space)**.** *Let X be a topological space. This time, we will consider the category slice category $\underline{\mathrm{Top}}/X$ whose objects are continuous maps $Y \to X$. We define a Grothendieck topology on $\underline{\mathrm{Top}}/X$ by saying that a family $\{(U_i \to X) \to (U \to X)\}$ is a covering if and only if the maps $f_i : U_i \to U$ define homeomorphisms between U_i and open subsets $f(U_i)$ of U, and if the $f(U_i)$ cover U.*

Remark 2.2.4 (the big site of all topological spaces)**.** In Example 2.2.3, one could drop X and simply consider the category of all topological spaces. On the other hand, if we take X to be a point, this is exactly what happens.

Example 2.2.5 (the Zariski site of (relative) schemes)**.** *Here we can let S be a scheme and consider the slice category $\underline{\mathrm{Sch}}/S$ of S-schemes. Following the idea of Example 2.2.3 we can define a Zariski cover $\{f_i : U_i \to U\}$ of S-schemes to be a family of maps of S-schemes such that the f_i are open immersions and the open sets $f_i(U_i)$ cover U.*

Example 2.2.6 (the big étale site of a scheme)**.** *Let S be a scheme and consider the slice category $\underline{\mathrm{Sch}}/S$ of S-schemes. Again following Example 2.2.3, we say that $\{f_i : U_i \to U\}$ is an étale cover of S-schemes when the maps f_i are étale and the open sets[1] $f_i(U_i)$ cover U.*

Example 2.2.7 (the small étale site of a scheme)**.** *Let S be a scheme and consider the subcategory of the slice category $\underline{\mathrm{Sch}}/S$ of S-schemes consisting only of étale morphisms to S. Again, we say that $\{f_i : U_i \to U\}$ is an étale cover of S-schemes when it is a cover in the sense of Example 2.2.6.*

Definition 2.2.8 (Morphisms of sites)**.** Let $(\mathcal{C}, \tau_{\mathcal{C}}), (\mathcal{D}, \tau_{\mathcal{D}})$ be sites. A morphism of sites $f : (\mathcal{C}, \tau_{\mathcal{C}}) \to (\mathcal{D}, \tau_{\mathcal{D}})$ is a functor $f^{-1} : \mathcal{D} \to \mathcal{C}$ such that for every cover $\{U_i \to U\} \in \tau_{\mathcal{D}}$, the family of morphisms $\{f^{-1}U_i \to f^{-1}U\}$ is in $\tau_{\mathcal{C}}$.

In particular, a continuous map of topological spaces $f : X \to Y$ induces a morphism of the corresponding sites via the actual inverse image $f^{-1} : Op(Y) \to Op(X)$. On the other hand, it need not be the case that a general map of sites should arise from a continuous map of topological spaces.

Remark 2.2.9 (Site morphism warning!)**.** The notation for sites and morphisms is an imperfect solution to an awkward problem. We would like to think of sites as akin to topological spaces, but the underlying categories have morphisms going in the opposite direction. For example, given sites $(\mathcal{C}, \tau_{\mathcal{C}})$ and $(\mathcal{D}, \tau_{\mathcal{D}})$, a morphism of sites $f : (\mathcal{C}, \tau_{\mathcal{C}}) \to (\mathcal{D}, \tau_{\mathcal{D}})$ might, with conventional abuse of notation $\mathcal{C} = (\mathcal{C}, \tau_{\mathcal{C}})$ and $\mathcal{D} = (\mathcal{D}, \tau_{\mathcal{D}})$ as $f : \mathcal{C} \to \mathcal{D}$, which starts to look very much like we are describing a functor between the underlying categories and not a morphism of sites. For this reason, one needs to be very careful to specify whether or not one is talking about a morphism in the sense of sites, or a functor on the underlying categories.

Definition 2.2.10 (Restriction)**.** Given a site $\mathcal{C} = (\mathcal{C}, \tau_{\mathcal{C}})$ and an object $U \in \mathcal{C}$, we define a new site $\mathcal{C}|_U$ to be the site whose underlying category is the slice category $\mathcal{C}{\downarrow}U$ of morphisms to U, and whose covers are those families $\{(V_i \to U) \to (V \to U)\}$ whose image $\{V_i \to V\}$ via the forgetful map to $\mathcal{C}$ is in $\tau_{\mathcal{C}}$.

[1] recall that étale morphisms are flat and finite presentation, hence open

Remark 2.2.11. The functor on underlying categories $\mathcal{C}\downarrow U \to \mathcal{C}$ gives a morphism of sites $\mathcal{C} \to \mathcal{C}|_U$, but this is not an intuitive geometric morphisms from the perspective of topological spaces in general (as it would correspond to a topological map of a space to an open subset).

On the other hand, given a morphism $V \to U$ in $\mathcal{C}$, we obtain a map $\mathcal{C}|_V \to \mathcal{C}|_U$ of sites which is the analog of "inclusion" of open sets. This works via sending $(W \to U)$ to $(W \times_U V \to V)$.

In particular if $\mathcal{C}$ itself has a terminal object $*$, one obtains a morphism of sites $\mathcal{C}|_U \to \mathcal{C}|_* = \mathcal{C}$ which is an analog of the inclusion of an open subset into an ambient space.

2.2.1 Sheaves on sites

Definition 2.2.12. Let $\mathcal{C}$ be a site and $\mathscr{F} : \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ a presheaf (=contravariant functor) with values in some other category $\mathcal{D}$. We say that $\mathscr{F}$ is a sheaf if for every cover $\{U_i \to U\}$, the natural map $\mathscr{F}(U) \to \prod \mathscr{F}(U_i)$ realize $\mathscr{F}(U)$ as the equalizer of the diagram

$$\prod_i F(U_i) \rightrightarrows \prod_{i,j} F(U_{i,j}).$$

Note that in particular, if $\mathcal{C}$ has an "empty set" in the sense of an object $\varnothing_{\mathcal{C}}$ for which the empty set is a cover of $\varnothing_{\mathcal{C}}$, then it would follow that for $\mathscr{F}$ a sheaf, $\mathscr{F}(\varnothing)$ would be a terminal object in $\mathcal{D}$ (so, for example, a singleton in Sets, the zero group in Abelian groups, or the zero ring in Rings).

Theorem/Exercise 2.2.13. *Sheaves satisfy descent. That is, for a site $\mathcal{C}$ and a covering $\mathscr{U} = \{\pi_i : U_i \to U\}$, the natural functor $\underline{\mathcal{S}\mathrm{hv}}_U \to \mathrm{Desc}(\mathscr{U}, \underline{\mathcal{S}\mathrm{hv}})$ given by $\mathcal{F} \mapsto ((\mathcal{F}|_i), (1_{i,j}))$ is an equivalence of categories.*

Proof idea. Verification of the fact that this map is fully faithful is relatively straightforward. For essential surjectivity, this amounts to extending a sheaf on a cover to a sheaf on the whole space U via application of the sheaf axiom of Definition 2.2.12 and then checking that this indeed defines a sheaf (i.e. that the sheaf axiom continues to hold on general covers). □

Remark 2.2.14. This idea can be extended to sheaves with extra structure – that is to say, the same result will hold when considering sheaves of groups, sheaves of Abelian groups, sheaves of rings, sheaves of modules or algebras over a given sheaf of rings, etcetera.

2.2.2 Stacks on sites

We begin with a notion which is a weak analog of a functor in a 2-categorical context. While we won't recall the full definition of a (strict) 2-category, we note the relevant structures for the 2-category $\underline{\mathfrak{C}\mathrm{at}}$ of categories, which are the horizontal and vertical compositions of natural isomorphisms.

For categories A, B, the collection of functors $F : A \to B$ themselves form a category, and the morphisms in this category are refered to as natural transformations. We use double arrows to denote these natural transformations as in $\alpha : F \Rightarrow G$. Composition in this category of functors we refer to as vertical composition. On the other hand, if we have categories A, B, C, functors $F, G : B \to C$ and $H : A \to B$ and a natural transformation $\alpha : F \Rightarrow G$, we obtain a natural transformation $\alpha \circ H : FH \to GH$, which we call the horizontal composition of α and H. As these can be notationally cumbersome, we will occasionally simply write α in place of $\alpha \circ H$.

Definition 2.2.15 (pseudofunctors)**.** Let C be a category. A psudofunctor from C valued in categories $\mathscr{S} : C \to \underline{\mathfrak{C}\mathrm{at}}$ is a rule which associates

1. to every object $U \in C$ a category $\mathscr{S}(U)$,
2. to every morphism $f : U \to V$ in C a functor $\mathscr{S}(f) : \mathscr{S}(U) \to \mathscr{S}(V)$,
3. to every pair of composable morphisms, $g : U \to V, f : V \to W$, a natural transformation $\mathscr{S}(f, g) : \mathscr{S}(f)\mathscr{S}(g) \Rightarrow \mathscr{S}(fg)$.

These should satisfy the following axioms:

(a) $\mathscr{S}(\mathrm{id}_U)$ coincides with the identity functor $\mathrm{id}_{\mathscr{S}(U)}$ on the category $\mathscr{S}(U)$,

should tihs be here??

(b) given a triple of composable maps $h : U \to V, g : V \to W, f : W \to Z$, we can apply $\mathscr{S}(f, g) \circ \mathscr{S}(h) : \mathscr{S}(f)\mathscr{S}(g)\mathscr{S}(h) \Rightarrow \mathscr{S}(fg)\mathscr{S}(h)$, followed by $\mathscr{S}(fg, h) : \mathscr{S}(fg)\mathscr{S}(h) \Rightarrow \mathscr{S}(fgh)$ to obtain natural transformation $\mathscr{S}(f)\mathscr{S}(g)\mathscr{S}(h) \Rightarrow \mathscr{S}(fgh)$. A similar natural transformation can be obtained by first applying $\mathscr{S}(f) \circ \mathscr{S}(g, h)$ and then $\mathscr{S}(f, gh)$. We require that these compositions coincide. That is, that:

$$\mathscr{S}(fg, h)\big(\mathscr{S}(f, g) \circ \mathscr{S}(h)\big) = \mathscr{S}(f, gh)\big(\mathscr{S}(f) \circ \mathscr{S}(g, h)\big)$$

as natural transformations from $\mathscr{S}(f)\mathscr{S}(g)\mathscr{S}(h)$ to $\mathscr{S}(fgh)$ between functors from U to Z.

Notation 2.2.16. Let C be a site and let $\{\pi_i : U_i \to U\}$ be a covering in C. We will use the notation $U_{i,j}$ to denote the fiber product $U_i \times_U U_j$ in C, and $U_{i,j,k}$ to denote $U_i \times_U U_j \times_U U_k$, and so on.

If $\mathscr{S} : C^{op} \to \underline{\mathfrak{C}\mathrm{at}}$ is a pseudofunctor, and $s \in \mathscr{S}(U)$, we will write $s|_i$ to denote $\mathscr{S}(\pi_i)(s)$. Similarly, if we write $\pi^i_{i,j}$ for the canonical map $U_i \times_U U_j \to U_i$, then for $s_i \in \mathscr{S}(U_i)$, we will write $s_i|_{i,j}$ to denote $\mathscr{S}(\pi^i_{i,j})(s_i)$, and so on.

Definition 2.2.17 (Descent data)**.** Let C be a site and let $\mathscr{S} : C^{op} \to \underline{\mathfrak{C}\mathrm{at}}$ be a pseudofunctor. Let $\mathscr{U} = \{\pi_i : U_i \to U\}$ be a covering in C. We define the descent category $\mathrm{Desc}(\mathscr{U}, \mathscr{S})$ to be the category whose objects are pairs $((s_i), (\phi_{i,j}))$ where each $s_i \in \mathscr{S}(U_i)$ and where $\phi_{i,j} : s_i|_{i,j} \to s_j|_{i,j}$ are isomorphisms such that for all i, j, k, we have

$$\phi_{i,k}|_{i,j,k} = \phi_{j,k}|_{i,j,k} \circ \phi_{i,j}|_{i,j,k}.$$

A morphism of descent data $f : ((s_i), (\phi_{i,j})) \to ((t_i), (\psi_{i,j}))$ consists of morphisms $f_i : s_i \to t_i$ which yield commutative diagrams:

$$\begin{array}{ccc} s_i|_{i,j} & \xrightarrow{\phi_{i,j}} & s_j|_{i,j} \\ {\scriptstyle f_i}\downarrow & & \downarrow{\scriptstyle f_j} \\ t_i|_{i,j} & \xrightarrow[\psi_{i,j}]{} & t_j|_{i,j}. \end{array}$$

Remark 2.2.18. If C is a site, $\mathscr{S} : C^{op} \to \underline{\mathfrak{Cat}}$ is a pseudofunctor, and $\mathscr{U} = \{\pi_i : U_i \to U\}$ be a covering in C, then we can define a functor

$$\epsilon : \mathscr{S}(U) \to \mathrm{Desc}(\mathscr{U}, \mathscr{S})$$

which is describe on objects as follows. Write $\pi_i : U_i \to U$, $\pi_{i,j} : U_{i,j} \to U$ and $\pi^i_{i,j} : U_{i,j} \to U_i$. For an object $s \in \mathscr{S}(U)$, we let $\epsilon(s) = (s|_i, 1_{i,j})$ where $1_{i,j} : s|_i|_{i,j} \to s|_j|_{i,j}$ denotes the canonical identification given as:

$$\begin{array}{ccccc} s|_i|_{i,j} & & \xrightarrow{\quad 1_{i,j} \quad} & & s|_j|_{i,j} \\ \| & & & & \| \\ \mathscr{S}(\pi^i_{i,j})\,\mathscr{S}(\pi_i)(s) & & & & \mathscr{S}(\pi^j_{i,j})\mathscr{S}(\pi_j)(s) \\ & {\scriptstyle \mathscr{S}(\pi^i_{i,j},\pi_i)(s)}\searrow & & \nearrow{\scriptstyle \mathscr{S}(\pi^j_{i,j},\pi_j)^{-1}(s)} & \\ & & \mathscr{S}(\pi_{i,j})(s) & & \end{array}$$

Definition 2.2.19 (stacks)**.** Let C be a site. We say that a pseudofunctor $\mathscr{S} : C^{op} \to \underline{\mathfrak{Cat}}$ is a stack if for every covering $\mathscr{U} = \{\pi_i : U_i \to U\}$ in C, the natural functor

$$\epsilon : \mathscr{S}(U) \to \mathrm{Desc}(\mathscr{U}, \mathscr{S})$$

from Remark 2.2.18 is an equivalence of categories.

Now, conventionally stacks are restricted to having images in groupoids instead of general categories, although this is not particularly essential.

Definition 2.2.20 (groupoids)**.** We say that a category G is a groupoid if each of its morphisms is invertible. Let $\underline{\mathfrak{Gpd}}$ be the sub 2-category of $\underline{\mathfrak{Cat}}$ consisting of groupoids.

Definition 2.2.21 (stacks (conventional definition))**.** Let C be a site. We say that a pseudofunctor $\mathscr{S} : C^{op} \to \underline{\mathfrak{Gpd}}$ is a stack if for every covering $\mathscr{U} = \{\pi_i : U_i \to U\}$ in C, the natural functor

$$\epsilon : \mathscr{S}(U) \to \mathrm{Desc}(\mathscr{U}, \mathscr{S})$$

from Remark 2.2.18 is an equivalence of categories.

2.2.3 The site of a stack

Given a site, we can now talk about the notion of stacks on the site. It turns out, that associated to any such stack is another site, which we can think of as analogous to the espace étale of a sheaf.

Definition 2.2.22. Let C be a site and let $\mathscr{S}$ be a stack on C. We can associate to $\mathscr{S}$ a site $s(\mathcal{S})$ which comes equipped with a functor $\mathfrak{s}(\mathcal{S}) \to C$. The objects of $\mathfrak{s}(\mathcal{S})$ are pairs (U, s) where $U \in C$ and $s \in \mathscr{S}(U)$. A morphism $(U, s) \to (V, t)$ is a pair (f, ϕ) consisting of a morphism $f \in \mathrm{Hom}_C(U, V)$ and an isomorphism $\phi : s \to \mathscr{S}(f)(t)$. We say that a family of morphisms $\{(U_i, s_i) \to (U, s)\}$ is a covering family if the collection $\{U_i \to U\}$ is a covering family in C. The functor $\mathfrak{s}(\mathscr{S}) \to C$ is given by $(U, s) \mapsto U$.

To motivate this definition, we should be thinking of $\mathscr{S}(f)(t)$ as playing the role of a pullback of t along the map $f : U \to V$ (in this analogy, we are thinking of s and t as representing, for example, families of schemes over U and V respectively). From this perspective, it is reasonable to denote $\mathscr{S}(f)(t)$ as $t|_U$. Intuitively, therefore, to find a morphism $s \to t$ which is compatible with the morphism $f : U \to V$ is equivalent to finding a map from s to the pullback $t|_U = \mathscr{S}(f)(t)$.

Remark 2.2.23 (Relation to fibered categories)**.** One may also define stacks using the equivalent formulation of fibered categories. While we won't go into this definition here, we note that for a stack $\mathscr{S}$ on a site C, the functor $\mathfrak{s}(\mathscr{S}) \to C$ has the structure of a fibered category, and will yield a stack via the standard definition in terms of such fibered categories.

2.3 Cohomology

Let C be a site. For an object $U \in C$, we obtain a functor $\Gamma_U : \underline{\mathrm{ab}\mathcal{S}\mathrm{hv}}_C \to \underline{\mathrm{Ab}}$ via $\Gamma_U(\mathscr{F}) = \mathscr{F}(U)$.

2.4 Ringed spaces and sites

Definition 2.4.1. A ringed space is a pair $X = (X, \mathcal{O}_X)$ where X is a topological space and $\mathcal{O}_X$ is a sheaf of rings on X. If Y is another ringed space, a morphism of ringed spaces $f = (f, f^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is the data of a continuous map $f : X \to Y$ together with a morphism of sheaves of rings $f^\# : \mathcal{O}_Y \to f_*\mathcal{O}_X$.

Recall that a homomorphism of local rings $\phi : R \to S$ is called a local homomorphism if $\phi(\mathfrak{m}_R) \subseteq \mathfrak{m}_S$ (or equivalently if $\phi^{-1}(\mathfrak{m}_S) = \mathfrak{m}_R$ as we assume ring homomorphisms are unital).

Definition 2.4.2. A locally ringed space is a ringed space X such that for every $x \in X$, the stalk $\mathcal{O}_{X,x}$ is a local ring. A morphism of locally ringed spaces is a morphism of ringed spaces $f : X \to Y$ such that the induced maps on stalks $\mathcal{O}_{Y,f(x)} \to f_*\mathcal{O}_{X,x}$ is a local homomorphism.

We'd like to consider not only ringed spaces – that is, sheaves of rings on topological spaces – but also ringed sites. For this there is an additionaly subtelty of not being able to refer to a notion of points and stalks.

Definition 2.4.3. A ringed site $C = (\mathcal{C}, \mathcal{O}_C)$ is a site $\mathcal{C}$ together with a sheaf of rings $\mathcal{O}_C$ on $\mathcal{C}$. A morphism of ringed sites $f : (\mathcal{C}, \mathcal{O}_C) \to (\mathcal{D}, \mathcal{O}_\mathcal{D})$ is a functor $f^{-1} : \mathcal{D} \to \mathcal{C}$

2.5 Etale (and general) Descent – twisted forms and obstructions

Let us now ask the same questions we asked before for étale covers, which we asked previously for Galois extensions. In fact, in light of Remark 2.2.14, we can really consider this in the context o a general site, perhaps with a sheaf of rings. We will ask this concretely in the context of quasicoherent sheaves of algebras over schemes with respect to the étale topology, and we will phrase things in this way, but we could also ask this for other types of algebraic structures over more general sites as well. So, suppose that $\{\pi_i : U_i \to U\}$ is an (étale) covering. We may ask the following questions:

Question 2.5.1. *Given a sheaf of $\mathcal{O}_U$ algebras $\mathcal{A}$, how can we describe all other sheaves of $\mathcal{O}_U$-algebras $\mathcal{A}'$ such that $\pi_i^*\mathcal{A} \cong \pi_i^*\mathcal{A}'$ for all i?*

Question 2.5.2. *Given sheaves of $\mathcal{O}_{U_i}$ algebras $\mathcal{B}_i$, when can we find a sheaf of $\mathcal{O}_U$ algebras $\mathcal{A}$ such that $\pi_i^*\mathcal{A} \cong B_i$ for each i?*

As before, we will write, for notational convenience, such things as $\mathcal{A}|_i$ for $\pi_i^*\mathcal{A}$.

Twisted forms and H^1

To answer Question 2.5.1, we note that by Theorem 2.1.3, it suffices to consider the following question: if we are given descent data $\mathcal{B}_\bullet = ((\mathcal{B}_i), (\phi_{i,j}))$ for an algebra with respect to the cover $\mathcal{U} = \{U_i \to U\}$, we need to consider what other possible descent data we are able to define. Before we proceed, let's make a quick notational comment:

Clarification 2.5.3 (Automorphisms of sheaves versus sheaves of autmorphisms)**.** Here when we have a sheaf of algebras $\mathcal{A}$ and we write $\mathrm{Aut}(\mathcal{A})$, what we mean is the group of automorphisms of the sheaf $\mathcal{A}$. That is, such an autormophism is a natural transformation of functors (i.e. a morphism of presheaves) $\mathcal{A} \to \mathcal{A}$. One may also consider the automorphsim sheaf $\mathscr{A}\mathrm{ut}$ which on some U is defined via $\mathscr{A}\mathrm{ut}(U) = \mathrm{Aut}(\mathcal{A}|_U)$. This should not be confused with the presheaf which associates to each U the group of automorphisms of the value of the

sections on U, $\mathrm{Aut}(\mathcal{A}(U))$. However, one can check that $\mathscr{A}\mathrm{ut}(\mathcal{A})$ is the sheafification of this presheaf and $\mathrm{Aut}(\mathcal{A})$ is the group of global sections of the sheaf $\mathscr{A}\mathrm{ut}(\mathcal{A})$.

Similarly, for sheaves of algebras $\mathcal{A}, \mathcal{A}'$ we can analogously define the sheaf of isomorphisms $\mathscr{I}\mathrm{so}(\mathcal{A}, \mathcal{A}')$ and its global sections $\mathrm{Iso}(\mathcal{A}, \mathcal{A}')$ consisting of "global isomorphisms."

In analogy to Definition 1.8.3, our descent data $\mathcal{B}_\bullet$ gives rise to descent data for its automorphisms – that is, we can define descent data $((\mathscr{A}\mathrm{ut}(\mathcal{B}_i)), (\mathscr{A}\mathrm{ut}(\phi_{i,j})))$ for a sheaf (and hence an étale sheaf by Theorem/Exercise 2.2.13 which we could call $\mathscr{A}\mathrm{ut}(\mathcal{B}_\bullet)$ as the sheaf $\mathscr{A}\mathrm{ut}(\mathcal{B}_i)$ on U_i and with

$$\mathrm{Iso}(\mathcal{B}_i|_{i,j}, \mathcal{B}_j|_{i,j}) \ni \mathscr{A}\mathrm{ut}(\phi_{i,j}) : \mathscr{A}\mathrm{ut}(\mathcal{B}_i)|_{i,j} \to \mathscr{A}\mathrm{ut}(\mathcal{B}_j)|_{i,j}$$

via for $V \to U_{i,j}$ and $f \in \mathrm{Aut}(\mathcal{B}_i)(V)$, we have $\mathrm{Aut}(\phi_{i,j})(V)(f) = \phi_{i,j}|_V f\, \phi_{i,j}^{-1}|_V$.

Note that in the case $\mathcal{B}_\bullet$ arises from a sheaf of $\mathcal{O}_U$-algebras $\mathcal{A}$, we would simply have that the descent data for $\mathcal{B}$ would be given by $((\mathcal{A}|_i), (\mathrm{id}_{\mathcal{A}|_{i,j}}))$ and $\mathrm{Aut}(\mathcal{B})$ would be given by $((\mathrm{Aut}(\mathcal{A}|_i)), (\mathrm{Aut}(\mathrm{id}_{\mathcal{A}|_{i,j}})))$ corresponding simply to the sheaf $\mathrm{Aut}(\mathcal{A})$. In fact, by Theorem 2.1.3, such an $\mathcal{A}$ always exists, so we can assume, without loss of generality, that $\mathcal{B}_\bullet$ has this form. This gives a significant notational simplification.

With this in mind, we can assume we start with a sheaf of algebras $\mathcal{A}$, and want to find all possible descent data of the form $((\mathcal{A}|_i), \psi_{i,j})$. In this context, $\psi_{i,j} \in \mathrm{Aut}(\mathcal{A}|_{i,j})$

Definition 2.5.4. For a sheaf of groups $\mathfrak{A}$ on a site C and a cover $\mathcal{U} = \{U_i \to U\}$, we define the pointed set $Z^1(\mathcal{U}, \mathfrak{A}) \equiv \{(\psi_{i,j}) \in \prod \mathfrak{A}(U_{i,j}) \mid \psi_{i,k} = \psi_{j,k}\psi_{i,j}\}$.

The following is essentially immediate from the defnitions:

Lemma 2.5.5. *Let $\mathcal{A}$ be a sheaf of algebras. Then we have a bijection between $Z^1(\mathcal{U}, \mathscr{A}\mathrm{ut}(\mathcal{A}))$ and descent data of the form $((\mathcal{A}_i), (\psi_{i,j}))$.*

In this way, we have parametrized all possible $\mathcal{A}'$ such that $\mathcal{A}'|_i \cong \mathcal{A}|_i$, however there is some amount of double counting. That is, we may have different descent datum $((\mathcal{A}_i), (\psi_{i,j}))$, $((\mathcal{A}_i), (\psi'_{i,j}))$ which are isomorphic (as descent data) and

2.6 (mostly March 27) Azumaya algebras over locally ringed spaces

In this section, we'll consider the notion of Azumaya algebras in the context of locally ringed spaces (or sites). So, suppose that X is a site (that is, a category equipped with a Grothendieck topology as in Definition 2.2.1), together with a sheaf of rings $\mathcal{O}_X$. In principle there may be many ways to try to define the notion of an Azumaya algebra over X. For example, we could say that it is a

sheaf of $\mathcal{O}_X$-algebras $\mathcal{A}$ such that the natural map $\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{A}^{\mathrm{op}} \to \mathscr{E}\mathrm{nd}_{\mathcal{O}_X}(\mathcal{A})$ is an isomorphism, or we could use one of the many other notions motivated by Proposition 1.4.14. In fact we will use one which was not part of our prior characterization of Azumaya algebras over rings (see Proposition 1.5.1), and it won't be until a bit later until we see that these notions are compatible (see **??**).

Definition 2.6.1 (Azumaya algebras over a ringed site)**.** Let $X = (X, \mathcal{O}_X)$ be a ringed site. We say that a sheaf of algebras $\mathcal{A}$ is Azumaya of rank n if for every object U in X, there exists a covering $\{U_i \to U\}$ such that the restriction $\mathcal{A}|_{U_i}$ is isomorphic to the sheaf of matrix algebras $\mathrm{M}_n(\mathcal{O}_X)$.

As before, we can define both a monoid structure on the collection of isomorphism classes of Azumaya algebras, and an equivalence relation which turns this monoid into a group. Recall that if X is a locally ringed space, a sheaf $\mathcal{V}$ of $\mathcal{O}_X$-modules is locally free of rank n if for every $U \in X$, there exists a covering $\{U_i \to U\}$ such that $\mathcal{V}|_{U_i} \cong \mathcal{O}_X^n$.

Definition 2.6.2. We define an equivalence relation on the isomorphism classes of Azumaya algebras, called Brauer equivalence to be the equivalence relation generated by the relation consisting of $\mathcal{A} \sim \mathcal{A} \otimes_{\mathcal{O}_X} \mathscr{E}\mathrm{nd}_{\mathcal{O}_X}(\mathcal{V})$ where $\mathcal{V}$ is a locally free sheaf of $\mathcal{O}_X$-modules of rank n for some n.

Definition 2.6.3 (Azumaya Brauer group)**.** For a ringed site X, we define the Azumaya Brauer group $\mathrm{Br}^{Az}(X)$ of X to be the set of Brauer equivalence classes $[\mathcal{A}]$ of Azumaya algebras $\mathcal{A}$ over X, with the operation $[\mathcal{A}] + [\mathcal{B}] = [\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{B}]$.

Verifying that this operation is associative and that $[\mathcal{O}_X]$ provides an additive identity element is straightforward. To see that we have inverses, we note that there is a canonical map

$$\mathcal{A} \otimes \mathcal{A}^{\mathrm{op}} \to \mathscr{E}\mathrm{nd}(\mathcal{A})$$

as before given by $a \otimes b \mapsto (x \mapsto axb)$. To finish, we need only check that this is an isomorphism of sheaves of algebras, which is to say that for every U, there exists a cover $\{U_i \to U\}$ such that the restriction of this map to U_i is an isomorphism. But by definition **??**, restricting to U_i allows us to assume that $\mathcal{A} \cong \mathscr{E}\mathrm{nd}(\mathcal{V})$ for some free $\mathcal{O}_X$-module $\mathcal{V}$. The result then follows from the observation that for any commutative ring R, the natural map

$$\mathrm{M}_n(R) \otimes \mathrm{M}_n(R) \to \mathrm{End}_R(\mathrm{M}_n(R)) = \mathrm{M}_{n^2}(R)$$

is an isomorphism. This in turn can be seen by observing the map on matrix units

$$e_{i,j} \otimes e_{k,\ell} \mapsto (e_{p,q} \mapsto \delta_{j,p}\delta_{k,q}e_{i,\ell})$$

which is to say that if we regard $M_{n^2}(R)$ as having matrix units $e_{(a,b),(c,d)}$ relative to a basis indexed by $\{1, \ldots, n\}^2$, we see this is described by

$$e_{i,j} \otimes e_{k,\ell} \mapsto e_{(i,\ell),(k,j)},$$

and hence is an isomorphism (as it takes an R-module basis to a R-module basis).

Definition 2.6.4 (Cohomological Brauer group)**.** Let X be a ringed site. The cohomological Brauer group $\mathrm{Br}^{Coh}(X)$ of X is defined to be the group $\mathrm{H}^2(X, \mathbb{G}_m)^{tors}$, that is, the torsion part of the second cohomology with coefficients in the multiplicative group.

To see how these groups relate to each other, we will need to consider the exact sequence

$$1 \to \mathbb{G}_m \to GL_n \to PGL_n \to 1,$$

and cohomology sequence

$$\mathrm{H}^1(X, \mathbb{G}_m) \to \mathrm{H}^1(X, GL_n) \to \mathrm{H}^1(X, PGL_n) \to \mathrm{H}^2(X, \mathbb{G}_m). \tag{2.1}$$

These sheaves of groups are defined as follows.

Definition 2.6.5. Let $X = (X, \mathcal{O}_X)$ be a ringed site. We define the sheaf of groups GL_n on X by $U \mapsto GL_n(\mathcal{O}_X(U))$, and $\mathbb{G}_m = GL_1$. We have a natural "diagonal" map $\mathbb{G}_m \to GL_n$ and we let PGL_n be the sheafification of the presheaf $U \mapsto GL_n(\mathcal{O}_X(U))/\mathbb{G}_m(\mathcal{O}_X(U))$. That is, PGL_n is the sheaf quotient $GL_n/\mathbb{G}_m$.

2.6.1 (Not from lecture) When is the projective general linear group a quotient?

Somewhat unintuitively, it need not be the case that $PGL_n(U) = GL_n(U)/\mathbb{G}_m(U)$. Indeed, we can understand this from examining aspects of the sequence (2.1). This will take us a bit to unpack though:

unpacking the exact sequence (2.1)

Via descent, we may interpret the pointed sets $\mathrm{H}^1(X, \mathbb{G}_m)$, $\mathrm{H}^1(X, GL_n)$ and $\mathrm{H}^1(X, PGL_n)$ by considering the groups $\mathbb{G}_m$, GL_n and PGL_n as sheaves of automorphisms. In particular, we find that $\mathbb{G}_m$ is the sheaf of automorphisms of $\mathcal{O}_X$ as a sheaf of modules over itself and GL_n is the sheaf of automorphisms of $\mathcal{O}_X^n$ as a sheaf of modules. Consequently, $\mathrm{H}^1(X, GL_n)$ is in bijection with isomorphism classes of sheaves of modules over $\mathcal{O}_X$ which are locally isomorphic to $\mathcal{O}_X^n$ – that is, locally free sheaves of rank n. In particular, $\mathrm{H}^1(X, \mathbb{G}_m)$ corresponds to locally free sheaves of modules of rank 1. The natural map $\mathbb{G}_m \to GL_n$ diagonally then can be interpreted as taking a locally free sheaf N of rank 1 to N^n, a locally free sheaf of rank n.

Let M_n denote the sheaf of matrix algebras given by $\mathrm{M}_n(U) = \mathrm{M}_n(\mathcal{O}_X(U))$. In favorable circumstances (for example for X a locally ringed space, as we will describe in Lemma 2.6.12 and Proposition 2.6.13), we will find that conjugation induces an identification of sheaves $PGL_n \cong \mathrm{Aut}(\mathrm{M}_n)$. We think about the map $GL_n \to PGL_n$ as taking an automorphism of R^n to the corresponding "change of basis" on its ring of linear transformations $\mathrm{M}_n(R)$. We can then show that the map from GL_n to PGL_n is given by associating to a locally free sheaf M of rank n, its endomorphism sheaf of algebras $\mathscr{E}\mathrm{nd}(M)$.

Definition 2.6.6. Let N be a sheaf of $\mathcal{O}_X$-modules. We say that N is n-free if $N^n \cong \mathcal{O}_X^n$.

The n-free line bundles form a subgroup of the Picard group – if P, Q are n-free then

$$(P \otimes Q)^n \cong P \otimes Q \otimes \mathcal{O}_X^n \cong P \otimes (Q \otimes \mathcal{O}_X^n) \cong P \otimes \mathcal{O}_X^n \cong \mathcal{O}_X^n,$$

and consequently, $P \otimes Q$ is n-free as well.

Definition 2.6.7. Let X be a ringed site. We let $Pic_{(n)}(X)$ denote the subgroup of $Pic(X)$ consisting of those locally free sheaves of rank 1 which are n-free. If R is a commutative ring, we similarly write $Pic_{(n)}(R)$ to denote $Pic_{(n)}(\operatorname{Spec} R)$. That is, isomorphism classes of projective R-modules N of rank 1 such that $N^n \cong R^n$.

Lemma 2.6.8. *For any ringed site X, $Pic_{(n)}(X)$ is n-torsion.*

Proof. Let $N \in Pic_{(n)}(X)$. Then $N^{\otimes n} \cong \Lambda^n N^n \cong \Lambda^n \mathcal{O}_X^n \cong \mathcal{O}_X$. □

Remark 2.6.9. As a partial converse to Lemma 2.6.8, it follows from the structure theory of modules over a Dedekind domain that $Pic_{(n)}(R)$ is exactly the n-torsion subgroup of $Pic(R)$ in the case that R is a Dedekind domain. Indeed, for a Dedekind domain, every projective module M is of the form $M \cong R^m \oplus P$ for some rank 1 projective module P. In particular, if $N \in Pic(R)$ is n-torsion, then if we write $N^n \cong R^{n-1} \oplus P$ and we find

$$R \cong N^{\otimes n} \cong \Lambda^n N^n \cong \Lambda^n (R^{n-1} \oplus P) \cong P,$$

and so $N^n \cong R^n$ which tells us that $N \in Pic_{(n)}(R)$ as claimed.

2.6.2 Relating the two Brauer group via Hilbert 90 spaces

We may attempt to define a map $\mathrm{Br}^{Az}(X) \to \mathrm{Br}^{Coh}(X)$ as follows. For an Azumaya algebra $\mathcal{A}$, we may consider $\mathcal{A}$ as a twisted form of the sheaf of $\mathcal{O}_X$-algebras $\mathrm{M}_n(\mathcal{O}_X)$. We would like to say that this is represented by a class in $\mathrm{H}^1(X, PGL_n)$ as would follow from the logic of Lemma 2.5.5. However, for this to work, we would need to know that the sheaf $\mathscr{A}\mathrm{ut}_{\mathcal{O}_X}(\mathrm{M}_n(\mathcal{O}_X))$ of automorphisms of matrix algebras is given by $PGL_n(\mathcal{O}_X)$ – that is, by conjugation. We knew that this was true in the case of fields by the Noether-Skolem theorem, however in general this is an extra assumption. For the purposes of the present conversation, we will make the following ad-hoc definitions:

Definition 2.6.10 (Hilbert 90 spaces)**.** We say that a ringed site X is a Hilbert 90 space if the presheaf $Pic(\mathcal{O}_X)$ given by $U \mapsto Pic(\mathcal{O}_X(U))$ is locally trivial (i.e. has trivial sheafification).

We can refine this slightly as follows:

Definition 2.6.11 (Hilbert 90(n) spaces)**.** We say that a ringed site X is Hilbert 90(n) space if the presheaf $Pic_{(n)}(\mathcal{O}_X)$ given by $U \mapsto Pic_{(n)}(\mathcal{O}_X(U))$ is locally trivial (i.e. has trivial sheafification). We say that X is a Hilbert 90 space if it is a Hilbert 90(n) space for all $n \in \mathbb{Z}_{\geqslant 1}$.

Now, if X is a locally ringed space, for example – that is, a topological space with a sheaf of rings $\mathcal{O}_X$ such that $O_{X,x}$ is a local ring for every point $x \in X$, then it is also a Hilbert 90 space, since projective modules over a local ring are free.

This will be a particularly useful concept for understanding the extent to which Noether-Skolem will apply for us, as the following Lemma illustrates:

Lemma 2.6.12. *Suppose $Pic(R) = 0$. Then the natural map $PGL_n(R) \to \mathrm{Aut}(\mathrm{M}_n(R))$ is an isomorphism.*

Proof. For the commutative ring R, the concept of rank of a projective module defines a function $\mathrm{Spec}(R) \to \mathbb{N}$.

Morita theory tells us that since R^n is a projective generator in the category of R-modules, we have an equivalence of categories between the category of R-modules and the category of $\mathrm{End}_R(R^n) = \mathrm{M}_n(R)$-modules, and this equivalence takes R to R^n. Let $\phi \in \mathrm{Aut}(\mathrm{M}_n(R))$. We see that if N is an R-module which is projective of rank r, then its image $R^n \otimes_R N$ is a projective $\mathrm{M}_n(R)$-module which, viewed as an R-module via the R-algebra structure of $\mathrm{M}_n(R)$, is a projective R-module of rank rn.

Precomposition with ϕ gives an auto-equivalence on the category of $\mathrm{M}_n(R)$-modules, where an $\mathrm{M}_n(R)$-module P is taken to a new module with structure given by $T \cdot p \equiv \phi(T)p$. As this is a categorical equivalence, it preserves categorical notions such as projectives and generators. Note that as every automorphism of $\mathrm{M}_n(R)$ preserves the R-algebra structure by definition, the R-module structure of modules is left unchanged.

In particular, we obtain two different $\mathrm{M}_n(R)$-module structures on R^n, the first being the standard one, and the second given by $T \cdot v = \phi(T)v$. Correspondingly, this second structure corresponds to an R-module N which is also a projective generator. Suppose N has rank r. Then it follows that R^n has rank rn as an R-module, which tells us that $r = 1$, or that N is a rank one projective module. As $Pic(R) = 0$, it follows $N \cong R$ which implies these two $\mathrm{M}_n(R)$-module structures determine isomorphic modules. Therefore we have an isomorphism $\psi : R^n \to R^n$ of R-modules such that

$$T \cdot \psi(v) = \psi(Tv)$$

or in other words, $\phi(T)\psi(v) = \psi(Tv)$ or $\phi(T) = \psi T \psi^{-1}$ as desired.

□

There is actually a bit more one could say here:

Proposition 2.6.13. *Let R be a commutative ring. Then the natural map $PGL_n(R) \to \mathrm{Aut}(\mathrm{M}_n(R))$ is an isomorphism if and only $Pic_{(n)}(R) = 0$.*

Proof sketch. Looking more carefully at the proof, one can see that the two $\mathrm{M}_n(R)$-module structures on R^n yield modules which are isomorphic as R-modules (by construction). Hence, by the explicit Morita equivalence, if the latter corresopnds to N as an R-module, then we must have an isomorphism $N^n \cong R^n$. So, in fact, we find the stronger conclusion that $PGL_n(R) \to \mathrm{Aut}(\mathrm{M}_n(R))$ is an isomorphism as long as there are no rank 1 projective R-modules N such that $N^n \cong R^n$.

Conversely, if we have such an N, and we choose an isomorphism $N^n \cong R^n$, we find that we obtain two corresponding $\mathrm{M}_n(R)$ module structures on R^n where via Morita theory, one corresponds to R and the other to N as R-modules. Hence these are different $\mathrm{M}_n(R)$-modules. However the isomorphism of R-modules $N^n \cong R^n$ induces an isomorphism of their endomorphism groups, which then gives an automorphism of $\mathrm{M}_n(R)$ which is cannot be given by conjugation. □

Proposition 2.6.14. *Let X be a Hilbert 90(n) space. Then we have an isomorphism of sheaves of groups:*

$$PGL_n(\mathcal{O}_X) \to \mathrm{Aut}(\mathrm{M}_n(\mathcal{O}_X))$$

The following Lemma now follows immediately from descent:

Lemma 2.6.15. *Suppose X is a Hilbert 90(n) space. Then we have a bijection between isomorphism classes of Azumaya algebras of rank n and the pointed set $\mathrm{H}^1(X, PGL_n)$.*

In this case, we obtain a map $\mathrm{Br}^{Az}(X) \to \mathrm{Br}^{Coh}(X)$ via the boundary map

$$\delta : \mathrm{H}^1(X, PGL_n) \to \mathrm{H}^2(X, \mathbb{G}_m).$$

need to explain why this lands in torsion still!

Lemma 2.6.16. *Let $\mathcal{A}, \mathcal{B}$ be Azumaya algebras over X. Then $\delta(\mathcal{A} \otimes \mathcal{B}) = \delta(\mathcal{A}) + \delta(\mathcal{B})$.*

It follows that the map is injective – if $\mathcal{A}$ has trivial class in $\mathrm{H}^2(X, \mathbb{G}_m)$, then it must be in the image of $\mathrm{H}^1(X, GL_n)$. But by our description of the sequence, it follows that we then would have $\mathcal{A} \cong \mathscr{E}\mathrm{nd}(\mathcal{V})$ for some locally free sheaf $\mathcal{V}$ of rank n. Hence $[\mathcal{A}] = 0$ in $\mathrm{Br}^{Az}(X)$.

Proposition 2.6.17. *Suppose X is a Hilbert 90(n) space for all n. Then we have an injective group homomorphism*

$$\mathrm{Br}^{Az}(X) \to \mathrm{Br}^{Coh}(X).$$

2.7 Spectral sequences: from Cech to Artin-Leray

There are many different spectral sequences we find in life, but in many ways, there are only a few from which all others are derived. Or perhaps there is only one. In any case, one candidate for such a "mother" spectral sequence is the Čech sequence. Let X be a site and $\mathscr{F}$ a sheaf of Abelian groups on $\mathscr{F}$ (or a sheaf in some appropriate Abelian category). This spectral sequence works as follows:

2.7.1 Čech combinatorics and simplicial objects

Given a covering $\{U_i \to U\}_{i\in I}$ in X, we can consider, for every ordered tuple of indices $i_\bullet = (i_0, i_1, \ldots, i_p)$ the iterated fiber product

$$U_{i_\bullet} = U_{i_0} \times_U U_{i_1} \times_U \cdots \times_U U_{i_p}$$

if we write $|i_\bullet| = p+1$ in the above situation, we can then set

$$U_p = \coprod_{|i_\bullet|=p+1} U_{i_\bullet}.$$

This collection comes with a natural collection of maps. For example, if

$$f : [p] = \{0, 1, \ldots, p'\} \to \{0, 1, \ldots p\} = [p]$$

is any map which preserves the partial order $\leqslant$, we see that for any tuple $i_\bullet$ with $|i_\bullet| = p+1$, if we let $f(i_\bullet) = (i_{f(0)}, i_{f(1)}, \ldots i_{f(p')})$, then there is a corresponding map on the fiber products in the other direction

$$U_{i_\bullet} \to U_{f(i_\bullet)}$$

(given by the universal property of fiber products). Proceeding this way for each index $i_\bullet$ with $|i_\bullet| = p+1$, we may put these together to obtain a map:

$$f^* : U_p \to U_{p'}.$$

In other words, if Δ is the category of finite, linearly ordered sets and order preserving maps (which can be taken, up to equivalence, to consist exactly of the objects $[p]$ and maps between them), then the rule

$$[p] \mapsto U_p$$

extends to a contravariant functor

$$U_\bullet : \Delta \to X^{\mathrm{op}}.$$

Composing this with the any presheaf $\mathscr{G}$, we obtain a covariant functor

$$\mathscr{G}(U_\bullet) : \Delta \to \underline{\mathrm{Ab}}$$

Definition 2.7.1. Let $\mathscr{C}$ be a category. A simplicial object in $\mathscr{C}$ is a contravariant functor $\Sigma : \Delta \to \mathscr{C}$. We write Σ_n for $\Sigma([n])$.

Definition 2.7.2. A cosimplicial object in $\mathscr{C}$ is a covariant functor $\Xi : \Delta \to \mathscr{C}$. We write Ξ_n for $\Xi([n])$ and we let $d_i : \Xi_{n-1} \to \Xi_n$ be defined as

$$d_{n,i} = \Sigma(\delta^{n,i} : [n-1] \to [n]),$$

where $\delta^{n,i}$ is the unique order preserving map which misses only the index $i \in [n]$. Let $d_n = \sum_{i=0}^{n} (-1)^i d_{n,i}$.

Definition 2.7.3. Let $\Xi : \Delta \to C$ be a cosimplicial object where C is an Abelian category. We define $\check{\mathrm{H}}^p(\Xi)$ to be the homology of the sequence

$$\Xi_{p-1} \xrightarrow{d_p} \Xi_p \xrightarrow{d_{p+1}} \Xi_{p+1}.$$

Let us come back to the situation where $\mathscr{F}$ is a sheaf of Abelian groups on a site X, and given our covering $\mathcal{U} = \{U_i \to U\}$ and corresponding cosimplicial object $U_\bullet$. We can define, for each $q \in \mathbb{N}$, a presheaf $\mathscr{H}^q(\mathscr{F})$ on X given by $\mathscr{H}^q(\mathscr{F})(V) = \mathrm{H}^q(V, \mathscr{F})$. Composing with the cosimplicial object $U_\bullet$ gives a simplicial object which we can concretely describe as:

$$\begin{aligned}\mathscr{H}^q(\mathscr{F})(U_\bullet) : \Delta &\to \underline{\mathrm{Ab}} \\ [p] &\mapsto \mathrm{H}^q(U_p, \mathscr{F}) = \prod_{|i_\bullet|=p} H^q(U_{i_\bullet}, \mathscr{F}).\end{aligned}$$

We finally can describe the Čech spectral sequence. Following convention we will write $\check{\mathrm{H}}^p(\mathcal{U}, \mathscr{H}^q(\mathscr{F}))$ for $\check{\mathrm{H}}^p(\mathscr{H}^q(\mathscr{F})(U_\bullet)$ below:

Proposition 2.7.4. *Let X be a site and $\mathscr{F}$ a sheaf of Abelian groups. Let $\mathcal{U} = \{U_i \to U\}$ be a covering. Then there is a convergent spectral sequence of cohomological type:*

$$\check{\mathrm{H}}^p(\mathcal{U}, \mathscr{H}^q(\mathscr{F})) \Rightarrow H^{p+q}(U, \mathscr{F}).$$

Proof. See [**?**, Tag 03OW]. □

2.7.2 From Čech covers to Galois covers

Suppose $\{\widetilde{X} \to X\}$ is a G-Galois covering of schemes. For a presheaf $\mathscr{G}$ on X, $\mathscr{G}(\widetilde{X})$ carries a G-action. Let $\widetilde{X}_\bullet$ be the cosimplicial scheme associated to this cover.

Proposition 2.7.5 (Artin-Leray Spectral Sequence)**.** *We have a natural isomorphism between Čech and Galois cohomology groups:*

$$\check{\mathrm{H}}^p(\mathscr{G}(\widetilde{X}_\bullet)) = H^p(G, \mathscr{G}(\widetilde{X})).$$

In particular, if we are given a Grothendieck topology within which $\{\widetilde{X} \to X\}$ is a covering, then we obtain a convergent spectral sequence

$$H^p(G, H^q(\widetilde{X}, \mathscr{F})) \Rightarrow H^{p+q}(X, \mathscr{F}).$$

Proof. TBD. □

Lemma 2.7.6. *Let $\widetilde{X} \to X$ be a G-Galois covering of S-schemes for a finite group G. Then we have an isomorphism $\widetilde{X} \times_X \widetilde{X} \cong \widetilde{X}^G$.*

Proof. Considering G as the S-group scheme S^G (a finite number of copies of S), we have a map

$$G \times \widetilde{X} \to \widetilde{X} \times \widetilde{X}$$

given by $(g \times x) \mapsto (x, gx)$ □

Chapter 3

Topics

3.1 The Brauer group and Picard group

In this section, we'll use the Artin-Leray spectral sequence (Proposition 2.7.5) to understand the behavior of the Picard group/functor/moduli problem. Let's start with the moduli problem itself. We consider the following:

Goal: parametrize line bundles on a smooth projective variety X.

Now, what should this goal exactly mean to us? At the basic level, given X a smooth projective variety over a field k, we'd like to construct a scheme $\mathcal{P}\mathrm{ic}_X$ whose k-points correspond to isomorphism classes of invertible sheaves on X. Unfortunately, it turns out that this is generally impossible, even for X a curve!

Before going further, it should be mentioned that a very excellent reference for understanding the Picard functor and its representability is the survey of Kleinman in [**?**].

Definition 3.1.1. Let X be a proper variety over a field k.

3.2 (mostly April 1) The Brauer group of a local ring

1. purity – Brauer group of punctured spectra in dimension > 1

3.3 The Brauer group of a complete discretely valued field (tame case)

1. Hensel's lemma and the correspondence between finite étale algebras (unramified extensions) over a Henselian dvr and its residue field
2. Existence of unramified splitting fields in the perfect case (and mention Kato cohomology / differential forms / crystalline ideas for the bad characteristic case)

3. The short exact ramification sequence

Theorem 3.3.1. *Let R be a complete discretely valued field with finite residue field, and let F be its field of fractions. Then we have a canonical isomorphism*

$$\mathrm{Br}(F) \cong \mathbb{Q}/\mathbb{Z}.$$

3.4 (April 8) Ramification, purity

-

more topics

3.5 Severi-Brauer schemes

The story of what are now known as Severi-Brauer (or as Brauer-Severi) schemes has as its origin the classification of genus 0 curves. As it is discussed in Châtelet's remarkable 1944 paper (see [**?**]), this problem had been considered by a number of authors, including Max Noether [**?**], David Hilbert and Adolf Hurwitz [**?**] in the late 1800, where it was shown that such a curve could always be described as a plane conic, and in particular was described by the solutions to a quadratic equation in three variables.

The question of considering when such curves had rational points was taken up by Poincare in 1901 [**?**] and then systematically investigated by Helmut Hasse [**?**] in 1935 where a close connection was made between such equations and the arithmetic of quaternion algebras.

In [**?**], François Châtelet introduced a vast generalization of these perspectives by introducing similar connections between certain higher dimensional varieties and general central simple algebras, which had been studied by Richard Brauer and many others at the time. For this reason, he called these varieties "variétés de Brauer" which we define below:

Definition 3.5.1. Let k be a field. We say that a k-variety X is a Severi-Brauer variety if $X_{\bar{k}} \cong \mathbb{P}^{n-1}_k$ for some n.

In order to give another characterization of Severi-Brauer varieties, let's recall the definition of the Grassmannian scheme.

Definition 3.5.2. Let S be a scheme and $\mathscr{F}$ a rank n locally free sheaf of $\mathscr{O}_S$-modules. We define the Grassmannian variety $\mathrm{Gr}(m, \mathscr{F})$ as representing the following functor. For an S-scheme T, we define:

$$\mathrm{Gr}(m, \mathscr{F})(T) = \{\text{rank } m \text{ subsheaves } \mathscr{E} \subset \mathscr{F}_T \mid \mathscr{F}_T/\mathscr{E} \text{ is locally free}\}.$$

Definition 3.5.3. Let S be a scheme and $\mathcal{A}/S$ a sheaf of Azumaya algebras over S of degree n. We define $X_{\mathcal{A}}$, the Severi-Brauer scheme associated to $\mathcal{A}$ as the S-scheme representing the following subfunctor of the Grassmannian.

$$X_{\mathcal{A}}(T) = \{\mathcal{I} \subset \mathrm{Gr}(n, \mathcal{A})(T) \mid \mathcal{I} \text{ is a sheaf of right ideals in } \mathcal{A}_T\}$$

3.6 Formal smoothness, etaleness

3.7 The Albert-Brauer-Hasse-Noether theorem

Theorem 3.7.1 (Alber-Brauer-Hasse-Noether)**.**

3.8 Gerbes and Azumaya algebras

We recall the notion of stacks from Section 2.2.2.

Definition 3.8.1. Let C be a site and $\mathscr{S}$ a stack on C. We say that $\mathscr{S}$ is a gerbe if

1. for every $U \in C$, there exists a cover $\{U_i \to U\}$ in C such that $\mathscr{S}(U_i) \neq \varnothing$ (that is, the category has at least one object), and,
2. for every $U \in C$, and $s, t \in \mathscr{S}(U)$, there exists a cover $\{U_i \to U\}$ in C such that $s|_i \cong t|_i$ for all i.

Definition 3.8.2. Let C be a site and μ a sheaf of Abelian groups on C. A μ-gerbe is a gerbe $\mathscr{S}$ on C together with, for every $U \in C$ and $s \in \mathscr{S}(U)$, together with a coherent system of isomorphisms $\mathfrak{a}_s : \mu(U) \xrightarrow{\sim} \mathrm{Aut}_{\mathscr{S}(U)}(s)$. More precisely, we ask that for every morphism $f : V \to U$ in C we have a commutative diagram (writing $s|V$ for $\mathscr{S}(f)(s)$),

can do this nicer by using the aut sheaf instead of the individual auts

$$\begin{array}{ccc} \mu(U) & \xrightarrow{\mathfrak{a}_s} & \mathrm{Aut}_{\mathscr{S}(U)}(s) \\ \downarrow & & \downarrow{\scriptstyle \mathscr{S}(f)(s)} \\ \mu(V) & \xrightarrow[\mathfrak{a}_{(s|V)}]{} & \mathrm{Aut}_{\mathscr{S}(V)}(s|_V), \end{array}$$

and for every morphism $\lambda : t \to u$ in $\mathscr{S}(U)$, we have a commutative diagram

$$\begin{array}{ccc} & \overset{\mathfrak{a}_t}{\nearrow} & \mathrm{Aut}_{\mathscr{S}(U)}(t) \\ \mu(U) & & \downarrow{\scriptstyle inn_\lambda} \\ & \underset{\mathfrak{a}_u}{\searrow} & \mathrm{Aut}_{\mathscr{S}(U)}(u), \end{array}$$

where inn_λ denotes the automorphism induced by conjugation.

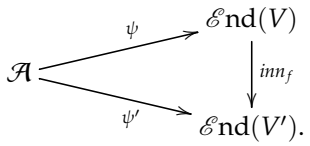
Proposition 3.8.3 (Giraud)**.** *Let C be a site and μ a sheaf of Abelian groups. Then we have a bijection of equivalence classes of μ-gerbes on C and the cohomology group $\mathrm{H}^2(C, \mu)$.*

3.8.1 Gerbes from Azumaya algebras

In this section we will describe how to pass from an Azumaya algebra to a gerbe.

Definition 3.8.4. Suppose X is a ringed site (as in Definition 2.6.11) and $\mathcal{A}$ is a sheaf of Azumaya algebras over X. We define a $\mathbb{G}_m$-gerbe $\mathcal{S}\mathrm{pl}_{\mathcal{A}}$ over X as follows. For $U \in X$, the objects of $\mathcal{S}\mathrm{pl}_{\mathcal{A}}(U)$ are pairs (V, ψ) consisting of a locally free sheaf V together with an isomorphism of sheaves of algebras $\psi : A \to \mathscr{E}\mathrm{nd}(V)$. A morphism $(V, \psi) \to (V', \psi')$ is the data of an isomorphism of sheaves $f : V \to V'$ such that if inn_f is the induced map $\mathscr{E}\mathrm{nd}(V) \to \mathscr{E}\mathrm{nd}(V')$

given by $T \mapsto fTf^{-1}$, then we have a commutative diagram:



Lemma 3.8.5. *Suppose X is a ringed site and $\mathcal{A}$ is an Azumaya algebra of rank n. Then $\mathcal{S}\mathrm{pl}_{\mathcal{A}}$ is a $\mathbb{G}_m$-gerbe over X.*

Proof. We note that scalar multiplication gives for every $(V, \psi) \in \mathcal{S}\mathrm{pl}_{\mathcal{A}}(U)$, a natural map $\mathbb{G}_m(U) \to \mathrm{Aut}(V)$ such that the corresponding inner automorphism is trivial. Hence this induces a map $\mathbb{G}_m(U) \to \mathrm{Aut}(V, \psi)$. We need only check that this is an isomorphism. But this follows from the fact that any $f : V \to V$ which gives an automorphism must be in the center of $\mathscr{E}\mathrm{nd}(V)$, and such an endomorphism is a scalar since it is a scalar when restricted to any open set $V \subseteq U$ on which V is trivial (this is from the fact that $\mathrm{Z}(M_n(R)) = R$ for any commutative ring R). □

3.9 Projective representations

This section consists of a more conversational summary of what I did in lecture on Monday, April 28.

3.9.1 Spin bundles

- first describe the idea of adding structure to a bundle via a representation
- so, given a vector bundle V/X, we may ask if we can endow V with the structure of a bilinear form?
- cohomology sequence here is the nonabelian one $O_n \to GL_n \to GL_n/O_n$ not a great interpretation or description here.
- but suppose we can do this. we can then ask about whether or not it has a well defined "volume form." or more precisely, can we lift to SO_n? Here the quotient is in $H^1(\pm 1)$ and so we actually get a double cover and ask how many sheets it has.
- if we can do this, we can actually ask if the bundle is spinnable. For this, it turns out that the group SO_n has a double cover $Spin_n$ (its the electron double spin thing) and we can do this if a brauer class vanishes.
- classical fact – this Brauer class is described via the clifford algebra of the quadratic form in the case of an even-dimensional form

3.9.2 central extensions vs gerbes

Given a group G over a field (or a sheaf of groups over a site X), we may ask for representations of G. These are, by definition, homomorphisms of the form $G \to GL_n$. But for various purposes, we are often more interested in projective representations $G \to PGL_n$. Unfortunately, there are generally much better tools for working with regular representations compared to projective ones – you can add them and multiply them, consider a K-group of them, etc.

central extensions

The conventional way of thinking about these is via central extensions. That is, given a projective rep $\rho : G \to PGL_n$ we can consider lifting along $GL_n \to PGL_n$ and considering the group $\widetilde{G}_\rho = \{(g, T) \in G \times GL_n \mid \rho(g) = \overline{T}\}$. This maps to G and is actually a central extension. Our projective representation of G now corresponds to a representation of $\widetilde{G}_\rho$. More or less conversely, if the corresonding representation $\widetilde{\rho} : \widetilde{G}_\rho \to GL_n$ is irreducible, it will follow that $Z(\widetilde{G}_\rho)$ maps to $Z(GL_n) = \mathbb{G}_m$ and consequently we will get back a projective rep of G from this.

We can do this for all projective reps at once by constructing (when we can) a universal central extension $\widehat{G} \to G$ which admits a map to each other universally $\widehat{G} \to \widetilde{G}_\rho$ and in particular a projective representation of G gives an ordinary representation of $\widehat{G}$. And as before, when the latter is irreducible we can go backwards.

In the prior section, we saw that lifting G bundles to $\widehat{G}$-bundles involves an H^2 obstruction, and this can often by lined up with a Brauer group computation.

projective reprentations and gerbes

The analogy with the prior section is not super tight, but let's try anyways.

We can also think about this somewhat stack-theoretically which allows us to consider it in families. So, suppose we have a site X (for example, corresponding to a complex analytic space with the standard complex topology). We suppose we have a sheaf of groups G on X and we are interested in a "family of projective representations." How could this work? We could imagine on a covering U_i of X, considering representations $\rho_i : G|_{U_i} \to GL_n = GL(V_i)$ with the ρ_i having some compatibility. How could this work? As we are working in families, we don't want the V_i to have to be constant, so they should at least locally look something like a vector bundle with identifications $\phi_{i,j} : V_i|_{ij} \to V_j|_{ij}$. On the other hand, we really just want things to be well defined when passing to $\overline{\rho}_i : G|_{U_i} \to PGL_n$, so we don't need that $\phi_{i,k} = \phi_{j,k}\phi_{i,j}$ on the nose, but rather just $\overline{\phi}_{i,k} = \overline{\phi}_{j,k}\overline{\phi}_{i,j}$ when considering representatitives in $PGL(V_i)$. In other words, we find that the $\overline{\phi}_{i,j}$ give gluing data for an Azumaya algebra of degree n, and our projective representation has its image in invertible elements of an Azumaya algebra instead of $GL(V)$ for some V.

But as it stands, this is a little less satisfying. We would like to regard our projective repesentations as honest representations in a somewhat different context. Here what we can do, is instead of changing the ring, we can change the space.

Namely, we can fiber this construction to the stack $\mathcal{S}\mathrm{pl}_{\mathcal{A}}$ if $\mathcal{A}$ is the Azumaya algebra described above. We then find that the V_i's now glue in the site of $\mathcal{S}\mathrm{pl}_{\mathcal{A}}$. More precisely, we can define a vector bundle V on $\mathcal{S}\mathrm{pl}_{\mathcal{A}}$ by describing, for each object (U, ψ) of $\mathcal{S}\mathrm{pl}_{\mathcal{A}}(U)$, which we can think of as an object of the site $\mathfrak{s}(\mathcal{S}\mathrm{pl}_{\mathcal{A}})$, we can consider the corresponding cover obtained by pulling back over the cover $\{U_i \to X\}$ – that is, the cover $\{(U_i \times_X U, \psi|_{U_i \times_X U}) \to (U, \psi)\}$ in $\mathfrak{s}(\mathcal{S}\mathrm{pl}_{\mathcal{A}})$. need to finish this

3.10 Brauer groups and Tate-Shafarevich groups

Here we take an interlude to consider the following problem: given a variety over the rational numbers or some other number field, when can we conclude that the variety has a rational point? In this generality, the problem is intractable, but what we would very much like is to be able to understand classes of varieties where such a determination could be made algorithmically.

Let's suppose we have some variety X over a number field k. We have previously seen, with the Brauer-Manin obstruction, the idea that one can determine in an algorithmic fashion whether or not $X(k_v)$ is nonempty where v is some valuation on k and k_v the corresponding completion. As we had previously considered, one can then consider the Brauer group of X, at least in cases where it is computationally accessible, in order to find potential new obstruction for rational points, assuming that $X(k_v) \neq \varnothing$ for all v.

Let us consider specifically the case where X is a smooth projective algebraic curve. In this case, we may ask how the problem of finding out whether or not a rational point exists relates to the genus of the curve. In the case that the curve is genus 0, we find that $X_{\bar{k}}$ is isomorphic to the projective line $\mathbb{P}^1_{\bar{k}}$, and consequently is the Severi-Brauer variety associated to a quaternion algebra Q (see Section 3.5). In this case, we find that $X(k) \neq \varnothing$ if and only if $Q \cong M_2(k)$. As we have seen from Theorem 3.7.1, $Q \cong M_2(k)$ if and only if $Q_{k_v} \cong M_2(k_v)$ for all v, or in other words, $X(k) \neq \varnothing$ if and only if $X(k_v) \neq \varnothing$ for all v. In particular, if X is genus 0, the Hasse principle holds, and we are able to determine whether or not X has a rational point by a deterministic algorithm, as the existence of local points is deterministically algorithmic.

On the other hand, the case when X has genus at least 2 (i.e. when X is general type or "hyperbolic"), has a very different kind of answer. By a result of Faltings, $X(k)$ is finite, and there are, in principle, effective bounds one may give for the number of points on such a curve. On the other hand, at present there is no known method for finding the points, or showing that the set of points is nonempty (although there are various methods which are effective for particular classes of curves).

This leaves us to the interesting case of genus 1, which is a kind of "sweet spot" computationally. In this case, we have been close for some time to finding effective answers, although a complete solution is still out of reach. Let us now describe the situation a bit.

Let X be a genus 1 curve over a field k. One then defines the Jacobian of X, written J_X to be the identity component of the Picard scheme for X. That is:

Definition 3.10.1. Let X be an algebraic curve over a field k. We define the Picard scheme of X, denoted Pic_X to be the sheafification of the presheaf on the étale site $k_{\text{ét}}$ given by

$$U \mapsto \mathrm{Pic}(X \times U).$$

Definition 3.10.2. For $d \in \mathbb{Z}$, we let Pic^d_X denote the subsheaf of Pic_X which associates to a k-scheme U the subset of $\mathrm{Pic}(X \times U)$ consisting of isomorphism classes of line bundles $\mathscr{L}$ over $X \times U$ such that for every $u \in U$, the restruction $\mathscr{L}|_{X \times u}$ is a degree 0 line bundle on the curve $X \times u$ (which is a curve over the residue field of the point u). We set $J_X = \mathrm{Pic}^0_X$ and call J_X the Jacobian of X.

Proposition 3.10.3. *Let X be a genus 1 curve. Then there is a canonical isomorphism $X \to \mathrm{Pic}^1_X$, which is described on L-points (for a field extension L/k) as $p \mapsto \mathcal{O}_{X_L}(p)$ for $p \in X(L)$.*

Proposition 3.10.4. *If X is a a genus 1 curve, then X is a principle homogeneous space (torsor) for the curve J_X regarded as a group scheme, and J_X is the unique elliptic curve (up to isomorphism) which admits X as a principle homogeneous space. Conversely, if $\mathcal{E}$ is any elliptic curve over k, then principal homogeneous spaces for $\mathcal{E}$ are genus 1 curves.*

- def of sha, conjectural finiteness
- brauer group vs weil-chatelet group
- regular model of the elliptic curve and brauer group of the model (Chebatarov)
- Brauer group = tate shafarevich group
- cassels-tate pairing (nondegenerate modulo divisible subgroup of sha)
- l-function of elliptic curve order of vanishing gives (conjecturally) the rank and the leading coefficient carries the information of sha
- sha is conjecturally finite by the above
- from Tanayama-Shimura, one now known finiteness of sha when analytic rank is at most 1

pairing as follows:

1. given a, a' in sha, consider X as the homogeneus space for a. Then a' gives a brauer class. This class is adically-locally constant, and the sum of the invariants of those constant classes is the value of the pairing.

Appendix A

Practice

A.1 semilinear spaces (the descent data category) with exercises

Exercise 1. If E/F is a G-Galois extension of fields, show that the natural map

$$\begin{aligned}(E, G, 1) &\to \mathrm{End}_F(E)\\ x &\mapsto [y \mapsto xy], \quad x, y \in E\\ u_\sigma &\mapsto [y \mapsto \sigma(y)], \quad \sigma \in G, y \in E\end{aligned}$$

gives an isomorphism of algebras.

Definition A.1.1. Recall that if E/F is a G-Galois extension, an E/F-semilinear vector space is an E-vector space V together with an action of G on V such that for every $x \in E$, $v \in V$, we have

$$\sigma(xv) = \sigma(x)\sigma(v).$$

A homomorphism of E/F semilinear vector spaces $\phi : V \to W$ consists of an E-linear map ϕ which commutes with the G-action in the sense that $\phi(\sigma v) = \sigma(\phi v)$.

Exercise 2. If V is an F-vector space then $E \otimes_F V$ is naturally an E/F semilinear vector space, where the action of G is via the first factor.

Exercise 3. Show that we have an equivalence of categories between $(E, G, 1)$-modules and E/F-semilinear vector spaces.

Recall the following result which we claimed in the last lecture:

Proposition A.1.2 (Morita)**.** *Let R be a ring and P a right R-progenerator (i.e. finitely generated, projective generator in the category of right R-modules). Let $S = \mathrm{End}_R(P)$. Then the functor from R-modules to S-modules given by*

$$N \mapsto P \otimes_R N$$

is an equivalence of categories. Further, if $P^\star = Hom_R(P, R)$ then $P^\star$ is an $R - S$ bimodule, and

$$M \mapsto P^\star \otimes_S M$$

gives the (homotopy) inverse equivalence.

Exercise 4. Show that the functor from F-vector spaces to E/F-semilinear vector spaces given by

$$V \mapsto V_E \equiv E \otimes_F V$$

is an equivalence of categories.

Now, if we are interested in talking about algebraic objects (such as central simple algebras), we need more than just vector spaces and linear maps, but we also need the concept of the tensor product (for multiplicative structures).

Definition A.1.3. Suppose V, W are E/F semilinear vector spaces. Then $V \otimes_E W$ is also a semilinear vector space with respect to the action:

$$\sigma(v \otimes w) = \sigma(v) \otimes \sigma(w).$$

Exercise 5. Show that the above definition gives a well defined E/F semilinear space and that this commutes with the functor given above.

That is, show that if V, W are F-vector spaces, then we have a natural isomorphism of E/F semilinear vector spaces

$$V_E \otimes_E W_E \cong (V \otimes_F W)_E.$$

More formally (if you like), this means you are showing that the two functors

$$(V, W) \mapsto (V_E \otimes_E W_E) \quad (V_W) \mapsto (V \otimes_F W)_E$$

from $Vec/F \times Vec/F$ to the category of E/F semilinear vector spaces are naturally isomorphic.

From this point of view it makes sense to talk about E/F semilinear algebras.

Definition A.1.4. An E/F semilinear algebra is an E/F semilinear vector space A, together with an E/F-semilinear map

$$m : A \otimes_E A \to A$$

and an E/F-semilinear map

$$\iota : E \to A$$

which gives A the structure of an algebra (where $\iota(1) = 1$ is the multiplicative identity of A).

Exercise 6. Show that an E/F semilinear algebra is just an E-algebra A with a semilinear action of G on A as a vector space such that $\sigma(ab) = \sigma(a)\sigma(b)$ (i.e. such that G acts via ring isomorphisms).

Exercise 7. Show that we have an equivalence of categories between F-algebras and E/F-semilinear algebras given by $A \mapsto E \otimes_F A$.

Exercise 8. It follows from the above exercise that if we let $F = \mathbb{R}$ and $E = \mathbb{C}$, then we have an equivalence between $\mathbb{R}$-algebras and $\mathbb{C}$-algebras with a notion of conjugation (action by $\mathcal{G}\mathrm{al}(\mathbb{C}/\mathbb{R})$). In particular, if we consider the $\mathbb{R}$-algebras $\mathbb{H}$ and $\mathrm{M}_2(\mathbb{R})$, we see that

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathrm{M}_2(\mathbb{C}) \cong \mathbb{C} \otimes_{\mathbb{R}} \mathrm{M}_2(\mathbb{R})$$

and so as $\mathbb{C}/\mathbb{R}$ semilinear algebras, both of these algebras are given as $\mathrm{M}_2(\mathbb{C})$ with two different notions of conjugation. What are these notions of conjugation?

A.2 twisted forms (the gluing problem) with exercises

Throughout the section, let us fix E/F a G-Galois extension.

Definition A.2.1. Let A be an F-algebra. We say that an F-algebra B is a(n E/F-)twisted form of A if there is an isomorphism of E-algebras, $A_E \cong B_E$.

Note that we are not assuming here that we have an isomoprhism of E/F semilinear algebras (which would imply they were isomorphic over F), but just as E-algebras.

As we saw in the previous section, we can recover the structure of B from B_E by specifying a semilinear action. As we are able to identify A_E and B_E, our quest to understanding the possible B's we may have then reduces to understanding all possible semilinear actions of G on A_E.

Definition A.2.2. Suppose V is a vector space with an action of G. We define an action of G on $\mathrm{Aut}(V)$ by $(\sigma\phi)(v) = \sigma(\phi(\sigma^{-1}(v))$.

Exercise 9. Show that in the case $V = E^n$, with component-wise action, the action of the Galois group $G = \mathcal{G}\mathrm{al}(E/F)$ on $Aut(V) = GL_n(E)$ is given by the standard action on the matrix entries.

Exercise 10. Suppose $\phi, \psi : G \to \mathrm{Aut}(A_E)$ are two different semilinear actions of G on A_E. That is, for $\sigma \in G$, we have $\sigma(a) \equiv \phi(\sigma)(a)$ and $\sigma(a) \equiv \psi(\sigma)(a)$ define semilinear actions (note here that ϕ and ψ need not have values in E-automorphisms, but in general just F-linear automorphisms).

Show that $\phi(\sigma) = \alpha(\sigma)\psi(\sigma)$ for a map $\alpha : G \to \mathrm{Aut}(A_E)$ and α is a crossed homomorphism (where the action of G on $\mathrm{Aut}(A_E)$ here is given by the previous excercise via ψ).

Exercise 11. Show that the above correspondence gives, after fixing an algebra A/F a bijection between semilinear actions on A_E and crossed homomorphisms $G \to \mathrm{Aut}_F(A_E)$.

From this we see so far that for B/F a twisted form of A, given an isomorphism $\phi : B_E \to A_E$, we obtain a new semilinear action on A_E which corresponds to the algebra B/F via the equivalence of categories previously described. This semilinear action, in turn gives rise to crossed homomorphism $G \to \mathrm{Aut}(A_E)$.

It therefore is natural to ask: in what way does this semilinear action depend on the isomorphism ϕ?

Bibliography

[Châ44] François Châtelet. Variations sur un thème de H. Poincaré. *Ann. Sci. École Norm. Sup. (3)*, 61:249–300, 1944.

[GS06] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Has35] Helmut Hasse. Elementarer Beweis des Hauptsatzes über ternäre quadratische Formen mit rationalen Koeffizienten. *J. Reine Angew. Math.*, 172:129–132, 1935.

[HH90] D. Hilbert and A. Hurwitz. Über die diophantischen Gleichungen vom Geschlecht Null. *Acta Math.*, 14(1):217–224, 1890.

[Kle05] Steven L. Kleiman. The Picard scheme. In *Fundamental algebraic geometry*, volume 123 of *Math. Surveys Monogr.*, pages 235–321. Amer. Math. Soc., Providence, RI, 2005.

[Noe84] M. Noether. Rationale Ausführung der Operationen in der Theorie der algebraischen Functionen. *Math. Ann.*, 23(3):311–358, 1884.

[Poi01] Henri Poincaré. Sur les propriétés arithmétiques des courbes algébriques. *Journal de mathématiques pures et appliquées*, 7(3):161–233, 1901.

[Sta24] The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2024.