Lecture Notes for MATH5051

(Taught by Prof. Jiu-Kang Yu)

Kyaw Shin Thant

December 12, 2023

The following are the lecture notes that I took during the class for MATH5051 (Abstract Algebra I) taught by Professor Jiu-Kang Yu at the Chinese University of Hong Kong during Fall 2023. These were slightly revised after the course ended. All typos and errors are solely my fault.

§ Lecture 1

The following is the course plan:

- Categories and functors
- Groups and categories
- Tensor products
- Galois theory of etale algebra over a field
- Semisimple algebras and Galois cohomology

There will be 5 exams, each 1 hour long, on

- September 14 (Basic category theory and group theory)
- October 5
- October 26
- November 9
- November 30

Definition 1.1. A *category* $\mathcal{C}$ consists of the following data:

(1) A collection (possibly a proper class) of objects $\mathrm{Ob}(\mathcal{C})$.

(2) For each pair $x, y \in \mathrm{Ob}(\mathcal{C})$ a set of morphisms $\mathrm{Mor}_{\mathcal{C}}(x, y)$.

(3) For each triple $x, y, z \in \mathrm{Ob}(\mathcal{C})$ a composition map $\mathrm{Mor}_{\mathcal{C}}(y, z) \times \mathrm{Mor}_{\mathcal{C}}(x, y) \to \mathrm{Mor}_{\mathcal{C}}(x, z)$, denoted $(\phi, \psi) \mapsto \phi \circ \psi$.

These data are to satisfy the following rules:

(1) For every element $x \in \mathrm{Ob}(\mathcal{C})$ there exists a morphism $\mathrm{id}_x \in \mathrm{Mor}_{\mathcal{C}}(x, x)$ such that $\mathrm{id}_x \circ \phi = \phi$ and $\psi \circ \mathrm{id}_x = \psi$ whenever the compositions make sense.

(2) Composition is associative, i.e., $(\phi \circ \psi) \circ \chi = \phi \circ (\psi \circ \chi)$ whenever these compositions make sense.

Example 1.1.1. Let Set be the category of all sets. Then $\mathrm{Ob}\,\mathsf{Set}$ is the *class* of all sets, $\mathrm{Mor}\,\mathsf{Set}$ is the class of functions between sets, and so on.

Definition 1.2. Let $\mathcal{C}$ be a category, and let $f \in \mathrm{Hom}_{\mathcal{C}}(C, D)$. We say that f is an *isomorphism* iff there exists $g \in \mathrm{Hom}_{\mathcal{C}}(D, C)$ such that $f \circ g = \mathrm{id}_D$ and $g \circ f = \mathrm{id}_C$.

Definition 1.3. Let $\mathcal{C}$ be a category and X be an object. We define its *automorphism group* $\mathrm{Aut}_{\mathcal{C}}(X)$ to be the isomorphisms in $\mathrm{Hom}_{\mathcal{C}}(X, X)$. This is really a group under morphism composition, as can be easily checked.

Definition 1.4. We say that X is an *initial object* of $\mathcal{C}$ if there is exactly one morphism from X to Y for any object Y in $\mathcal{C}$. We say that X is a *final object* if there is exactly one morphism from Y to X for all Y.

Lemma 1.1. *Initial/final objects, if they exist, are unique up to unique isomorphism.*

Proof. Let X and X' be two initial objects. Then there is a unique morphism from X to X', say f, and similarly a unique morphism f' from X' to X. They are inverse of each other because $f \circ f'$ is an element of $\mathrm{Hom}_{\mathcal{C}}(X, X)$, which is a singleton whose only element is the identity. Therefore, $f \circ f' = \mathrm{id}_{X'}$ and $f' \circ f = \mathrm{id}_X$. □

Example 1.4.1. In Set, the initial object is the empty set and the final object is any singleton. In Grp, both the initial and final objects are the trivial group. In Ring, the initial object is $\mathbb{Z}$ and the final object is the trivial ring.

Here is another example of a category.

Example 1.4.2. Let A and B be two sets. We can form a category $\mathcal{C}$ as follows. The objects of this category are triples (P, f, g) where P is a set and f and g are functions from P to A and B respectively. The morphism set between two triples (P, f, g) and (P', f', g') is the set of maps $\phi : P \to P'$ such that $f' \circ \phi = f$ and $g' \circ \phi = g$.

Lemma 1.2. *This category has an final object, which is the* cartesian product $(A \times B, f, g)$ *where f and g are respective projections.*

Proof. Given any object (P, f', g'), there is exactly one morphism from P to $A \times B$, defined by $\phi(x) = (f'(x), g'(x))$ for all $x \in P$. □

The point is that we can do this construction for any category $\mathcal{C}$. We can no longer guarantee that such a final object exists anymore, but when it does, we can define

Definition 1.5. If such an object exists, then we say that it is the *product* of A and B.

Example 1.5.1. In the category of topological spaces, the product of two objects A and B exists. The underlying set is just the cartesian product $A \times B$, and the topology is the product topology.

Definition 1.6. Let $\mathcal{C}$ be a category. We define a new category $\mathcal{C}^{\mathrm{op}}$ which is called the opposite category of $\mathcal{C}$ simply by reversing all the arrows. To be more exact, the objects of $\mathcal{C}^{\mathrm{op}}$ are the same as that of $\mathcal{C}$. The hom set $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(X, Y)$ is the same as $\mathrm{Hom}_{\mathcal{C}}(Y, X)$. The composition is defined by reversing everything: $f \circ_{\mathrm{op}} g \coloneqq g \circ f$.

This exhibits a duality, in that a final object of $\mathcal{C}$ corresponds to an initial object of $\mathcal{C}^{\mathrm{op}}$.

Definition 1.7. Let Q be the product of A and B in the opposite category. Then we call Q the *coproduct* of A and B in $\mathcal{C}$.

Example 1.7.1. The coproduct of A and B in Set is the disjoint union of A and B. The coproduct of two abelian groups A and B is the usual direct product of A and B. The coproduct of topological spaces is their disjoint union.

Example 1.7.2. In Grp, the coproduct exists, but it is non-trivial compared to other examples. Given two groups A and B, the coproduct is the *free product* of A and B, denoted as $A * B$.

Question. Show that $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z} = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$.

Proof. See here. The main idea is Euclidean Algorithm. Looking at the action of a matrix on other matrices is also very useful. □

For some references on category theory, Professor Yu recommended Lang's *Algebra*, and Mac Lane's *Categories for the working mathematician*.

§ Lecture 2

Definition 2.1. Let $\mathcal{C}$ and $\mathcal{C}'$ be two categories. A *functor* $\mathcal{F}$ from $\mathcal{C}$ to $\mathcal{C}'$ is a map which sends each object $X \in \mathcal{C}$ to an object $\mathcal{F}(X) \in \mathcal{C}'$, and each morphism $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ to a morphism $\mathcal{F}(f) \in \mathrm{Hom}_{\mathcal{C}'}(\mathcal{F}(X), \mathcal{F}(Y))$. Moreover, it is compatible with composition and identity morphisms.

Example 2.1.1. As a mundane example, we can define a functor from Grp to Set by forgetting the group structure.

Example 2.1.2. Similarly, we can define a functor $\mathcal{F}$ from Ring to Grp by simply forgetting the multiplicative structure of the ring and only looking at the underlying abelian group with addition. We can also define another functor by mapping each ring to its multiplicative group.

Example 2.1.3. Let's try to define a 'functor' $\mathcal{C}$ from Top to Ring. For each topological space X, we can define $\mathcal{C}(X)$ to be the space of continuous real-valued functions, which can be given a natural ring structure by adding and multiplying them pointwise. Now let's say $f : X \to Y$ is a continuous map between topological spaces. Then we can define a map $\mathcal{C}(f)$ from $\mathcal{C}(Y) \to \mathcal{C}(X)$ by simply composing with f on the right. However, note that everything is actually reversed; even the composition law is $\mathcal{C}(f) \circ \mathcal{C}(g) = \mathcal{C}(g \circ f)$. We say that $\mathcal{C}$ is a *contravariant* functor from Top to Ring. More precisely, it is a functor from $\mathsf{Top}^{\mathrm{op}}$ to Ring.

Example 2.1.4. Let $\mathcal{M}$ be the category of pointed manifolds, i.e., its objects are pairs (X, x) such that X is a differentiable manifold and $x \in X$. The morphisms between (X, x) and (Y, y) are differentiable maps from X to Y such that x is mapped to y. We can define a functor $\mathcal{C}$ from $\mathcal{M}$ to $\mathsf{Vect}(\mathbb{R})$ by mapping each (X, x) to the tangent space at X. Note that each differentiable map $f : X \to Y$ defines a map between the respective tangent spaces via the differential. By chain rule, this is a functor.

Example 2.1.5. Let $\mathcal{C}$ be a category whose objects are (G, N) where G is a group and N is a normal subgroup of G. The morphisms between (G, N) and (G', N') are the homomorphisms from G to G' taking N inside N'. We can now define a functor $\mathcal{Q}$ from $\mathcal{C}$ to Grp by the quotient map. This is well-defined because of the universal property of quotients; the kernel of the quotient map $G' \to G'/N'$ is N', so composition with $f : G \to G'$ results in a map whose kernel contains N. This induces a unique map from G/N to G'/N' via the universal property.

Example 2.1.6. We can define a functor from Ring to Ring by mapping R to $R[x]$. We can also define another functor by mapping R to $M_n(R)$.

Now let's move on to natural transformations.

Definition 2.2. A *natural transformation* α from $\mathcal{F}$ to $\mathcal{F}'$ consists of a collection of morphisms $\alpha_X : \mathcal{F}(X) \to \mathcal{F}'(X)$ for each object X, such that if f is a morphism from X to Y, $\alpha_Y \circ \mathcal{F}(f) = \mathcal{F}'(f) \circ \alpha_X$.

Let $\mathrm{Fun}(\mathcal{C}, \mathcal{C}')$ be all functors from $\mathcal{C} \to \mathcal{C}'$. We can make this into a category in the following way. The objects of this category are the functors $\mathcal{C} \to \mathcal{C}'$. If $\mathcal{F}$ and $\mathcal{F}'$ are in $\mathrm{Fun}(\mathcal{C}, \mathcal{C}')$, we define $\mathrm{Mor}(\mathcal{F}, \mathcal{F}')$ to be the set of natural transformations from $\mathcal{F}$ to $\mathcal{F}'$. Composition of natural transformations is defined pointwise.

Example 2.2.1. Let's take the category from Example 2.1.5. We can define another functor $\mathcal{F}$ by forgetting the group N, i.e., mapping (G, N) to G. Then we can define a natural transformation α by letting $\alpha_{(G,N)}$ to be the quotient map from G to G/N.

Example 2.2.2. We can define a functor GL_n from $\mathsf{CommRing}$ to Grp by mapping R to $\mathrm{GL}_n(R)$. We can also define a functor GL_1 by mapping R to $R^\times$. Then there exists a natural transformation between two functors, which is just the determinant map det.

Example 2.2.3. The functor d which maps a vector space V to its dual $V^\vee$ is a contravariant functor. We can compose it with itself to have a functor $d \circ d$. Then there is a natural transformation between the identity function id and $d \circ d$. Of course, this is just the canonical isomorphism (in the case of finite-dimensional vector spaces) that we get by feeding $v \in V$ to elements of $V^\vee$ to make an element of the double dual $(V^\vee)^\vee$.

Definition 2.3 (Yoneda embedding)**.** Let $\mathcal{C}$ be any category. Let $\mathrm{Fun}(\mathcal{C}, \mathsf{Set}^{\mathrm{op}})$ be the category of contravariant functors from $\mathcal{C}$ to Set. Then we can define a functor h from the original category $\mathcal{C}$ to $\mathrm{Fun}(\mathcal{C}, \mathsf{Set}^{\mathrm{op}})$. For each object $X \in \mathcal{C}$, we map it to a functor h_X which is defined as follows: for each object Y in $\mathcal{C}$, $h_X(Y)$ is defined to be the set $\mathrm{Hom}_{\mathcal{C}}(Y, X)$. For each map $f : Y_1 \to Y_2$, we define $h_X(f) : \mathrm{Hom}(Y_2, X) \to (Y_1, X)$ by composing maps in $\mathrm{Hom}(Y_2, X)$ with f on the right.

§ Lecture 3

Let's continue with the Yoneda embedding. We have associated with each object X of $\mathcal{C}$ a contravariant functor h_X from $\mathcal{C}$ to Set. Now we do the same thing for morphism between objects of $\mathcal{C}$. Suppose that we have a map $f : X \to Y$. Then we associate with it a natural transformation $h_f : h_X \to h_Y$ which is defined as follows: for any object $Z \in \mathcal{C}$, we define the component of h_f, denoted as $h_{f,Z}$ by mapping $h_X(Z) = \mathrm{Hom}(Z, X)$ to $h_Y(Z) = \mathrm{Hom}(Z, Y)$ by composing with f on the left. It is easy to check that this is indeed a natural transformation. Now all that's left to check is that this association is indeed a functor. This is not too hard, so I'll just leave this to my future self.

We can now state a very important result in category theory.

Lemma 3.1 (Yoneda). *h is fully faithful, i.e., the map*

$$\mathrm{Hom}_{\mathcal{C}}(X, X') \to \mathrm{Hom}_{\mathrm{Fun}(\mathcal{C}, \mathsf{Set}^{op})}(h_X, h_{X'})$$

is a bijection.

Proof. Let's first show that this map is injective. Assume that f_1 and f_2 are morphisms to X to X', and suppose that the associated natural transformations h_{f_1} and h_{f_2} are the same. We wish to show that $f_1 = f_2$. Remember that for any object Y and $\phi : Y \to X$, $h_{f_1}(\phi) = f_1 \circ \phi$. Therefore, if we take Y to be X and ϕ to be id_X, then $f_1 = h_{f_1}(\phi) = h_{f_2}(\phi) = f_2$.

The heart of the lemma is that this map is also surjective. Suppose that we have a natural transformation α from $h_X \to h_{X'}$. We have to show that there exists a morphism $f : X \to X'$ such that $\alpha = h_f$. Of course, if it exists, then it would be equal to $\alpha_X(\mathrm{id}_X)$, so we let f to be this element. We want to show that $\alpha = h_f$.

Let Y be any object of $\mathcal{C}$, and let g be an element of $h_X(Y) = \mathrm{Hom}(Y, X)$. We want to check that $\alpha_Y(g) = \alpha_X(\mathrm{id}_X) \circ g$. This follows from the naturality of α, since

$$\alpha_Y(g) = \alpha_Y(h_X(g)(\mathrm{id}_X)) = h_{X'}(g)(\alpha_X(\mathrm{id}_X)) = \alpha_X(\mathrm{id}_X) \circ g. \qquad \square$$

Now we want to discuss the equivalence of categories. Suppose that $\mathcal{C}$ and $\mathcal{D}$ are categories, and let $\mathcal{F}$ and $\mathcal{G}$ be functors from $\mathcal{C}$ to $\mathcal{D}$ and vice versa. The naive way to say that $\mathcal{C}$ and $\mathcal{D}$ are isomorphic would be if $\mathcal{F}$ and $\mathcal{G}$ induce bijections between objects and morphisms. This turns out to be a bit too restrictive. Instead, we make the following definition.

Definition 3.1. Suppose that $F \circ G$ and $\mathrm{id}_{\mathcal{D}}$ are isomorphic as elements of $\mathrm{Fun}(\mathcal{D}, \mathcal{D})$, and similarly for $G \circ F$ and $\mathrm{id}_{\mathcal{C}}$. Then we say that $\mathcal{C}$ and $\mathcal{D}$ are *equivalent categories* and that $\mathcal{F}$ and $\mathcal{G}$ are *equivalence functors.*

Here are some examples.

Example 3.1.1. Let $\mathsf{fVect}_{\mathbb{R}}$ denote the category of finite dimensional vector spaces over $\mathbb{R}$. Let $\mathcal{C}$ be the full subcategory (hom sets are just the ones from the original category.) consisting of the objects $\mathbb{R}^n$ where $n \geq 0$. Let i be the obvious functor $\mathcal{C} \to \mathsf{fVect}_{\mathbb{R}}$. Then i is an equivalence functor.

To show this, we need to find a functor $\mathcal{G}$ in the other direction. For each object $V \in \mathsf{fVect}_{\mathbb{R}}$, we can choose an isomorphism $\phi_V : V \to \mathbb{R}^{\dim V}$. Now we define the functor $\mathcal{G}$ by $\mathcal{G}(V) = \mathbb{R}^{\dim V}$ For any morphism $f \in \mathrm{Hom}(V, W)$, we define $\mathcal{G}(f)$ to be $\phi_W \circ f \circ \phi_V^{-1}$. This definition is intentionally made so that $\mathcal{G}$ satisfies the properties of a functor.

Now let's check that i is indeed an equivalence functor. Note that $(\mathcal{G} \circ i)(\mathbb{R}^n)$ is just $\mathbb{R}^n$. Therefore,

$$(\mathcal{G} \circ i)(f) = \mathcal{G}(f) = \phi_{\mathbb{R}^m} \circ f \circ \phi_{\mathbb{R}^n}^{-1}.$$

It is easy to see that the natural transformation α given by $\alpha_{\mathbb{R}^n} = \phi_{\mathbb{R}^n}$ is indeed a natural transformation from $\mathcal{G} \circ i \to \mathrm{id}_{\mathcal{C}}$. The other direction can be checked similarly.

Here is another characterization of equivalence.

Theorem 3.2. *A functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ is an equivalence functor if and only if $\mathcal{F}$ is fully faithful and essentially surjective. (The latter means that for any object Y in $\mathcal{D}$, there exists an object in $\mathcal{C}$ such that $\mathcal{F}(X)$ is isomorphic to Y.)*

§ Lecture 4

We will discuss about tensor products in this lecture. Let M be an abelian group. Then $\mathrm{Hom}(M, M)$ has a ring structure with pointwise addition and composition as multiplication.

Definition 4.1. Let A be a ring. Then a *left A-module* is (M, α), where M is an abelian group, and $\alpha : A \to \mathrm{Hom}(M, M)$ is a ring homomorphism.

Usually, we surpress α, and write $\alpha(a)(m)$ as am. We can think of this as an analog of group action, but here the underlying object is an abelian group instead of a set.

Given a ring A, we can consider its opposite ring. Then a *right A-module* is just a left A^{op}-module.

Remark. There's one fundamental difference between group actions and modules. For every group G, $G \cong G^{\mathrm{op}}$ naturally, so we can always convert a left G-action into a right G-action. However, in the case of rings, $A \ncong A^{\mathrm{op}}$ in general. Therefore, there is no obvious way to turn a left A-module into a right A-module. Some important examples of the nice case when $A \cong A^{\mathrm{op}}$ are

- A is a commutative ring
- $A = k[G]$ is a group algebra where k is commutative
- $A = M_n(k)$ where k is a commutative ring.

[*Slight digression*]

Question. What are all the isomorphisms between $M_n(k)$ and $M_n(k)^{\mathrm{op}}$? Are there any other isomorphism except for transpose?

To answer this question, we recall a useful fact: if $\mathcal{C}$ is a category with objects X and X', and if there exists an isomorphism from X to X' in $\mathcal{C}$, then the set of isomorphisms is a principal homogeneous space of $\mathrm{Aut}(X')$. In other words, once there exists a single isomorphism, the others are just composition of that isomorphism with automorphisms of X'.

Theorem 4.1. *If k is a field,*

$$\mathrm{Aut}(M_n(k)) = \{\mathrm{conj}(g) : g \in GL_n(k)\}$$

where $\mathrm{conj}(g)$ *is conjugation by* g.

Corollary 4.1.1. $g \in \mathrm{GL}_n(k) \mapsto (g^t)^{-1}$ *is an automorphism of* $\mathrm{GL}_n(k)$ *(or* $\mathrm{SL}_n(k)$*). In fact,* $\mathrm{Aut}_k(\mathrm{SL}_n(k))/\mathrm{Inn}(\mathrm{SL}_n(k))$ *is a group of order* 2.

[*Digression ends*]

Let A be a ring, let M_A be a right A-module, and ${}_AN$ be a left A-module.

Definition 4.2. Let L be an abelian group. A map $\phi : M \times N \to L$ is called *A-bilinear* if $\phi(m, -) : N \to L$ is an abelian group homomorphism for all $m \in M$, and similarly for $\phi(-, n)$, and moreover, $\phi(ma, n) = \phi(m, an)$.

Let $\mathrm{BiHom}(M \times N, L)$ be the set of A-bilinear maps $\phi : M \times N \to L$. We can now define the tensor product of right and left A-modules as follows using a universal property.

Fix M and N. We form a category $\mathcal{C}$, where the objects of $\mathcal{C}$ are tuples (ϕ, L) where L is an abelian group and ϕ is A-bilinear. The morphisms between (ϕ, L) and (ϕ', L') are just abelian group homomorphisms $\alpha : L \to L'$ which satisfies $\alpha \circ \phi = \phi'$.

Definition 4.3. This category $\mathcal{C}$ has an initial object. If (ϕ_0, L_0) is an initial element of $\mathcal{C}$, then we denote L_0 as $M \otimes_A N$, and $\phi_0(m,n)$ as $m \otimes n$. We say that L_0 is the *tensor product* of M and N over A.

Of course, we still have to show that $\mathcal{C}$ indeed has an initial object. This is a classic construction.

Proof. Let T be the free abelian group $M \times N$. By definition, T has a basis $\{e_{m,n}\}_{(m,n)\in M\times N}$. Now consider the subgroup of T generated by elements of the form

$$e_{m,n+n'} - e_{m,n} - e_{m,n'}, e_{m+m',n} - e_{m,n} - e_{m',n}, \quad \text{and} \quad e_{ma,n} - e_{m,an},$$

and denote it by R. Now we define L_0 to be T/R, and the map $\phi_0 : M \times N \to L_0$ by $\phi(m,n) = e_{m,n} + R$. It is obvious that ϕ_0 is A-bilinear.

Now suppose that L is an abelian group, and ϕ is an A-bilinear map from $M \times N \to L$. If there is a homomorphism $f : L_0 \to L$ such that $f \circ \phi_0 = \phi$, then $f(e_{m,n} + R) = (m,n)$ for all (m,n). Since $e_{m,n}$ span T, such an f must be unique. We now show the existence. Viewing ϕ as a map of sets, ϕ induces a unique abelian group homomorphism ϕ' from the free group T to L. The kernel of this group homomorphism contains R, so by the universal property of quotients, this again induces a unique group homomorphism ϕ'' from $L_0 = T/R$ to L. □

Remark. $\otimes$ is a functor from $\mathsf{Mod}_A \times {}_A\mathsf{Mod} \to \mathsf{Ab}$. In particular, if we have $\alpha : M \to N$ and $\beta : M' \to N'$, then we have a map $(\alpha, \beta) : M \times M' \to N \times N'$, and by the functorial property, we must have a map $\alpha \otimes \beta : M \otimes M' \to N \otimes N'$, which takes $m \otimes n$ to $\alpha(m) \otimes \beta(n)$.

§ Lecture 5

We can say that $M \otimes_A N$ co-represents the functor $\mathsf{Ab} \to \mathsf{Set}$ which maps L to the set of A-bilinear maps from $M \times N \to L$.

Definition 5.1. A functor $\mathcal{F} : \mathcal{C} \to \mathsf{Set}^{\mathrm{op}}$ is called *representable* if $F \cong h_X$ for some h_X in the image of Yoneda embedding.

Now consider a variant of the embedding $\mathcal{C}^{\mathrm{op}} \to \mathrm{Fun}(\mathcal{C}^{\mathrm{op}}, \mathsf{Set}^{\mathrm{op}})$. The right side is just $\mathrm{Fun}(\mathcal{C}, \mathsf{Set})$, so we have a contravariant functor from $\mathcal{C}$ to $\mathrm{Fun}(\mathcal{C}, \mathsf{Set})$.

Definition 5.2. A functor is called *co-representable* if it is in the image of this opposite Yoneda embedding.

Note that until now, there is no natural way to define a module structure on $M \otimes_A N$. We can change that by imposing extra conditions on M and N.

Definition 5.3. Let A, B be rings. An (A, B)-bimodule is a left $(A \times B^{\mathrm{op}})$-module.

Usually, for an (A, B)-bimodule, we regard M as both a left A-module and a right B-module such that the two actions commute, i.e., $(am)b = a(mb)$. We denote this structure by ${}_AM_B$.

Lemma 5.1. *Let M be an (A, B)-bimodule, and let N be a (B, C)-bimodule. Then the abelian group $M \otimes_B N$ can be given a natural (A, C)-bimodule structure.*

Proof. Since M is an (A, B)-bimodule, left multiplication by an element of A gives a right B-module endomorphism of M. Similarly, since N is a (B, C)-bimodule, right multiplication by an element of A gives a left B-module endomorphism of N. If we have a right B-module endomorphism ϕ of M, and a left B-module endomorphism τ of N, then it can be checked that the map

$$\begin{aligned} M \times N &\to M \otimes N \\ (m, n) &\mapsto \phi(m) \otimes \tau(n) \end{aligned}$$

is B-bilinear, hence induces an abelian group endomorphism of $M \otimes_B N$ which maps $m \otimes n \to \phi(m) \otimes \tau(n)$. In particular, by the previous observation, it follows that an element of $A \times C^{\mathrm{op}}$, say (a, c), gives an abelian group endomorphism of $M \otimes_B N$, by mapping $m \otimes n \to am \otimes nc$. Note that

$$((a, c) \cdot (a', c'))(m \otimes n) = (a, c)(a'm \otimes nc') = aa'm \otimes nc'c = (aa', c \cdot_{\mathrm{op}} c')(m \otimes n)$$

which shows that this map is a ring homomorphism to $\mathrm{End}_{\mathsf{Ab}}(M \otimes_B N)$. This completes the proof. □

As a generalization, we can check that ${}_BM_A \otimes_A N_C$ corepresents the functor from the category of (B, C)-bimodules to Set, which maps each object L to the set of A-bilinear maps from ${}_BM_A \times {}_AN_C$ to L which are also (B, C)-linear.

Remark. If we're working in the category of left A-modules, then $\mathrm{Hom}({}_AM, {}_AN)$ is an abelian group. Also, $\mathrm{Hom}({}_AM_B, {}_AN_C)$ is a right $(B \times C)$-module.

We now want to define the tensor product of algebras.

Definition 5.4. Let A be a commutative ring. An *A-algebra* is a pair (α, R) such that $\alpha : A \to R$ is a ring homomorphism, with $\alpha(A)$ lying in the center of R. In other words, $\alpha(a)r = r\alpha(a)$ for all $a \in A$ and $r \in R$. We write ar to denote $\alpha(a)r$.

In particular, the multiplication defined above gives the ring R an (A, A)-bimodule structure. Note that the condition that $\alpha(A)$ lies in the center of R implies that the multiplication map $R \times R \to R$ is A-bilinear.

Theorem 5.2. *If B and C are A-algebras, then $B \otimes_A C$ has a canonical A-algebra structure.*

We list some preliminary facts.

1. $M \otimes N \cong N \otimes M$ and this isomorphism maps $m \otimes n$ to $n \otimes m$. (Note that we require commutativity of A here as otherwise one of the tensor products above will be undefined!)
2. $M \otimes (N \otimes L) \cong (M \otimes N) \otimes L$, and this isomorphism maps $m \otimes (n \otimes \ell)$ to $(m \otimes n) \otimes \ell$.

Proof. Of course, we already have an (A, A)-bimodule structure on $B \otimes_A C$. Therefore, we just need to define a multiplication, which is an A-bilinear map from $(B \otimes C) \times (B \otimes C) \to B \otimes C$. This is the same as constructing an abelian group homomorphism $(B \otimes C) \otimes (B \otimes C) \to B \otimes C$. By the two facts above, the left side is isomorphic to $(B \otimes B) \otimes (C \otimes C)$. Now the rest is easy. We have an A-linear map $B \otimes B \to B$ by multiplication, and similarly, we have an A-linear map $C \otimes C \to C$ by mutliplication. Therefore, by the functorial property, we can construct an abelian group homomorphism $(B \otimes B) \otimes (C \otimes C) \to B \otimes C$ which maps $(b \otimes b') \otimes (c \otimes c')$ to $bb' \otimes cc'$. Reversing our steps, this gives us a bilinear map from $(B \otimes C) \times (B \otimes C) \to B \otimes C$ which maps $(b \otimes c, b' \otimes c')$ to $bb' \otimes cc'$. This is exactly the multiplication map that we desire. It is easy to check that this map satisfies all properties of multiplication that we need (associativity, distributivity, etc.) □

Similarly to the tensor product of modules, we can also characterize the tensor product of algebras via a universal property.

Definition 5.5. Fix A-algebras B and C. Form a category $\mathcal{C}$ whose objects are diagrams consisting of a map $\beta : B \to R$ and another map $\gamma : C \to R$, and $\beta(b)$ commutes with $\gamma(c)$ for all $b \in B$ and $c \in C$. For any two diagrams, the set of morphisms between them is just the set of morphisms from $R \to R'$ that makes the diagram commute.

Theorem 5.3. *This category has an initial object, which is the tensor product of B and C.*

In particular, the tensor product of B and C is the coproduct in the category of commutative A-algebras. This is because the extra commutativity condition in the construction above is automatically satisifed for commutative A-algebras.

We are quite far from the ground now, so let's try to look at some specific examples and basic facts.

Fact 5.1. *$M \otimes_A N$ is generated by the subset $\{m \otimes n : m \in M, n \in N\}$. These are called* simple tensors*.*

Fact 5.2. *If $I \subset A$ is a two-sided ideal, then A/I is a right A-module and we can tensor it with M. This turns out to be isomorphic to M/IM where $IM = \{\sum i_s m_s : i_s \in I, m_s \in M\}$.*

Proof. We have a map from $(A/I) \times M \to M/IM$ defined by $(a + I, m) \to am + IM$. This map is A-bilinear, so it gives a map $\alpha : (A/I) \otimes_A M \to M/IM$. Now define a map from $M \to (A/I) \otimes_A M$ defined by $m \to (1 + I) \otimes m$. The kernel of this map contains IM, so this gives a map from $\beta : M/IM \to (A/I) \otimes_A M$ which maps $m + IM \to (1 + I) \otimes m$. It is now easy to check that α and β are inverses of each other. □

Lemma 5.4. *Tensor product also distributes over direct sum.*

$$\left(\bigoplus_{i\in I} M_i\right) \otimes_A N \cong \bigoplus_{i\in I} (M_i \otimes_A N).$$

§ Lecture 6

A corollary of the preceeding lemma is that if M is a free right A-module with basis $\{e_i\}_{i\in I}$, then $M \otimes_A N \cong \bigoplus_{i\in I} N$. In particular,

Lemma 6.1. *If both M and N are free A-modules, where A is commutative, then $M \otimes_A N$ is also a free A-module. If M has basis $\{e_i\}$ and N has basis $\{f_j\}$, then $M \otimes_A N$ has basis $\{e_i \otimes f_j\}$.*

Suppose that A is commutative, and that B and C are A-algebras. Assume that C is free as an A-module with basis $\{e_i\}_{i\in I}$. Then

$$B \otimes_A C = \bigoplus_{i\in I} B \otimes_A (Ae_i)$$

as A-modules. We want to investigate its ring structure as well. By definition, $(b\otimes e_i)(b'\otimes e_j) = bb'\otimes (e_ie_j)$. We can then write e_ie_j as a linear combination of the basis e_i which gives the corresponding image in the direct sum on the right hand side.

Example 6.0.1. Let $C = A[x]$ be a polynomial ring where A is commutative, and let $\{e_i\} = \{1, x, x^2, \ldots\}$. Then

$$B \otimes_A C = \bigoplus_{i=0}^{\infty} B \otimes_A (Ax^i).$$

From this, it can be seen that $B \otimes_A C$ is just $B[x]$. As a generalization, if f is a monic polynomial of degree n and $C = A[x]/(f)$, then C is a free A-module of degree n. Then

$$B \otimes_A \frac{A[x]}{fA[x]} \cong \frac{B[x]}{fB[x]}.$$

Example 6.0.2. $B\otimes_A M_n(A) \cong M_n(B)$. This is because $M_n(A)$ is the free A-module with generators $\{e_{ij}\}_{1\le i,j\le n}$ satisfying $e_{ij}e_{kl} = \delta_{jk}e_{il}$. Therefore, $B \otimes_A M_n(A)$ is a free B-module with generators that satisfy the same relation. Therefore, it must be isomorphic to $M_n(B)$. In general, $M_n(A) \otimes_A M_m(A) = M_{nm}(A)$.

Let A be an arbitrary ring, and let M, N be left A-modules. Then we can define

$$M^\vee \coloneqq \mathrm{Hom}(M, A),$$

and since A is an (A, A)-bimodule, the above has a right A-module structure. Then there is a natural bilinear map

$$\Phi : M^\vee \times N \to \mathrm{Hom}(M, N), \quad (\phi, n) \mapsto (m \mapsto \phi(m)n).$$

which gives an abelian group homomorphism from $M^\vee \otimes_A N \to \mathrm{Hom}(M, N)$. In fact, this gives a natural transformation between the two functors from ${}_A\mathsf{Mod} \times_A \mathsf{Mod}$ to Ab the first of which maps $(M, N) \mapsto M^\vee \otimes_A N$ and the second which maps $(M, N) \mapsto \mathrm{Hom}(M, N)$.

The map $\alpha_{M,N}$ is an isomorphism when M is free of finite rank. Since the two functors commute with direct sums, we just need to prove this proposition for the case when the rank is 1. This can be checked easily.

In particular, if M is free of finite rank over A, then

$$\mathrm{End}_A(M) \cong M^\vee \otimes_A M.$$

However, observe that the left hand side is a ring. This means that we can impose a natural ring structure on $M^\vee \otimes_A M$ corresponding to this. For simplicity, assume that A is commutative. Let $\phi \otimes m$ and $\tau \otimes n$ be two elements of $M^\vee \otimes_A M$. Then

$$(\phi \otimes m)(x) = \phi(x)m \quad \text{and} \quad (\tau \otimes n)(x) = \tau(x)n$$

when viewed as elements of $\mathrm{End}_A(M)$. Since the product operation in the latter is composition, the product of the above two maps is

$$x \mapsto \phi(\tau(x)n)m = \tau(x)\phi(n)m.$$

The element of $M^\vee \otimes_A M$ corresponding to this is $\tau \otimes \phi(n)m$.

If A is a commutative ring and M and N are free A-modules, then $\mathrm{End}_A(M)$ and $\mathrm{End}_A(N)$ are A-algebras. By the above, there exists an abelian group homomorphism

$$\mathrm{End}_A(M) \otimes_A \mathrm{End}_A(N) \cong M^\vee \otimes M \otimes N^\vee \otimes N \cong (M \otimes N)^\vee \otimes (M \otimes N) \cong \mathrm{End}_A(M \otimes N).$$

Fact 6.1. *The above is in fact an isomorphism of A-algebras.*

Proof. Denote the map by Φ. We need to check two things: first that ϕ is a ring homomorphism, and that ϕ is an A-module homomorphism. The latter is not too hard, so we will only prove the first one. Let $f \in \mathrm{End}_A(M)$ correspond to elementary tensor $\phi \otimes m$, and $g \in \mathrm{End}_A(N)$ correspond to $\tau \otimes n$. Then the image of $f \otimes g$ under Φ is

$$f \otimes g \mapsto \phi \otimes m \otimes \tau \otimes n \mapsto (\phi \otimes \tau) \otimes m \otimes n,$$

and so

$$\Phi(f \otimes g)(x \otimes y) = \phi(x)\tau(y)(m \otimes n).$$

Since ff' corresponds to $\phi' \otimes \phi(m')m$, and gg' corresponds to $\tau' \otimes \tau(n')n$, we have

$$\Phi(ff' \otimes gg')(x \otimes y) = \phi'(x)\tau'(y)(\phi(m')m \otimes \tau(n')n) = \phi'(x)\phi(m')\tau'(y)\tau(n')(m \otimes n),$$

and

$$(\Phi(f \otimes g) \cdot \Phi(f' \otimes g'))(x \otimes y) = \Phi(f \otimes g)(\phi'(x)\tau'(y)(m' \otimes n')) = \phi'(x)\tau'(y)\phi(m')\tau(n')(m \otimes n)$$

which shows that Φ is multiplicative for preimages of elementary tensors. Since $\mathrm{End}_A(M) \otimes \mathrm{End}_A(N)$ is generated by such tensors and Φ is linear, it follows that Φ is multiplicative for all elements. It is now easy to check that Φ is a ring homomorphism. □

§ Lecture 7

[All the modules in this lecture are left modules unless specified otherwise.]

Let $\phi : A \to B$ be a ring homomorphism. Then any B-module N can be regarded as an A-module. Denote this A-module by $\phi^* N$. Then ϕ^* is a functor from the category of B-modules to the category of A-modules. We now want to do the reverse: given any A-module M, we want to give a nice B-module structure to M.

For any A-module M, we can consider the tensor product $B \otimes_A M$ which also has a B-module structure as well. In this way, we get another functor ϕ_* which takes A-modules to B-modules. This construction is called *base change*.

Fact 7.1. *ϕ_* is left adjoint to ϕ^*.*

Proof. Suppose that we have a map $f : M \to N$, where M is an A-module and N is a B-module. Then we can define a map from $B \times M \to N$ by mapping $(b, m) \to bf(m)$. Then this is A-bilinear, so this induces a map $\alpha(f) : B \otimes_A M \mapsto N$. For the other direction, if $g : B \otimes_A M \to N$, then we can define $\beta(g) : M \to N$ by mapping $m \mapsto g(1 \otimes m)$. This gives two maps:

$$\alpha : \mathrm{Hom}_{A-\mathsf{Mod}}(M, \phi^* N) \to \mathrm{Hom}_{B-\mathsf{Mod}}(\phi_* M, N),$$

and β in the opposite direction. It can be checked that α and β are inverses to each other. □

Now let's assume that A and B are commutative rings. We can do the exact same construction as above between the category of A-algebras and that of B-algebras.

Example 7.0.1. Suppose that H is a subgroup of G, and k is a field. Then we can consider the k-algebra $k[H]$, whose elements are formal linear combinations of elements of H with coefficients in k. Then we have an inclusion $\phi : k[H] \to k[G]$. Then we have a bijection between sets

$$\{k[G]\text{-modules}\} \leftrightarrow \{\text{representations of } G \text{ on a } k\text{-vector space}\}.$$

We have a map ϕ^* from G-representations to H-representations by restriction. As before, we can construct a map ϕ_* from H-representations to G-representations. In this context, our construction is called the Frobenius reciprocity law.

There are many other pairs of interesting adjoint functors. Here is an example.

Example 7.0.2. Let A be a commutative ring, and let M and N be A-modules. If we fix an A-module L, then an A-linear map from $M \otimes_A L \to N$ is the same as an A-linear map from $M \to \mathrm{Hom}(L, N)$. Therefore, the functor $- \otimes_A L$ is left adjoint to $\mathrm{Hom}(L, -)$. From this adjointness property, we see that $- \otimes_A N$ and $M \otimes_A -$ are right exact functors.

Before we can start discussing about the Galois theory of etale algebras, we will quickly go through the basics of classical Galois theory. Let k be a field.

Definition 7.1. Let $f \in k[x]$. Then f is *separable* if $\gcd(f, f') = 1$ in $k[x]$. This definition avoids using an explicit algebraic closure, but it just means that f does not have roots of multiplicity greater than 1.

Fact 7.2. *Let $f, g \in k[x]$, and let E be any field extension of k. Then $\gcd(f, g)$ in $k[x]$ is the same as $\gcd(f, g)$ in $E[x]$.*

Fact 7.3. $f(x) \equiv f(a) + (x - a)f'(a) \pmod{(x - a)^2}$.

These two facts show that this definition of separability agrees with our intuition.

Corollary 7.0.1. *If $f \in k[x]$ is separable, then f is separable in $E[x]$ for any extension E of k, and f does not have a double root in E.*

Definition 7.2. Let $\alpha \in E$. We say that α is *separable* over k if the irreducible polynomial of α is separable.

From this, we immediately get the following:

Corollary 7.0.2. *If* $\operatorname{char} k = 0$*, any $\alpha \in E$ is separable.*

Proof. Let f be the irreducible polynomial of α over k. Since $\operatorname{char} k = 0$, this implies that f' is a non-zero polynomial of degree strictly less than f. Hence $\gcd(f, f') = 1$ and α is separable. □

Separable irreducible polynomials do exist in non-zero characteristic.

Lemma 7.1. *Assume that* $\operatorname{char} k = p$*. Let $g \in k[x]$ be a monic irreducible polynomial. Then there exists a monic irreducible separable polynomial g_0 and an exponent $e \geq 0$ such that $g(x) = g_0(x^{p^e})$ and this pair is uniquely determined by g.*

Sketch. If g is irreducible but not separable, then $g' = 0$, so $g(x) = h(x^p)$ for some h. Now induct. □

Definition 7.3. An algebraic extension E/k is called *separable* if every element $\alpha \in E$ is separable over k.

Definition 7.4. Suppose that E/k is algebraic and $\alpha \in E$. Then α is called *purely inseparable* if $\alpha^{p^n} \in k$ for some $n \geq 0$. This is equivalent to the fact that the irreducible polynomial of α is of the form $x^{p^m} - a$ where $a \in k$.

Definition 7.5. Let $\overline{k}$ be the algebraic closure of k. Then the perfect closure of k is defined as

$$k^{\mathrm{perf}} = k^{\frac{1}{p^\infty}} = \{\alpha \in \overline{k} \mid \alpha \text{ is purely inseparable}\}.$$

This is independent of the choice of $\overline{k}$, in the following sense; if $\overline{k}'$ is another algebraic closure, then there exists an isomorphism $\phi : \overline{k} \to \overline{k}'$. This induces an isomorphism of the perfect closures, and this isomorphism is independent of the choice of ϕ.

We can view this closure in another way. If k is a field of characteristic p, then k^{perf} is the inverse limit of the tower where the maps are Frobenius endomorphisms.

Theorem 7.2 (Mac Lane)**.** *Let k be a field of characteristic p, and let E be an algebraic extension. Then TFAE:*

(1) E is separable over k.

(2) The map $E \otimes_k k^{perf} \to E^{perf}$ is injective.

(3) $E \otimes_k k^{perf}$ is reduced.

(4) $E \otimes_k k'$ is reduced for any field extension k' of k.

The condition (2) can be rephrased as E and k^{perf} are linearly disjoint in E^{perf}.

Definition 7.6. Let L/k be a field extension, and let E and F be intermediate fields. We say that E and F are *linearly disjoint* in L if $E \otimes_k F \to L$ is injective.

Lemma 7.3. *E and F are linearly disjoint in L iff for any $e_1, \dots, e_n \in E$ which are linearly independent over k, then $e_1, \dots, e_n$ are linearly independent over F.*

Proof. Suppose that $E \otimes_k F \to L$ is injective, and let $e_1, \dots, e_n \in E$ be linearly independent over k. Suppose that there exist $f_1, \dots, f_n \in F$ such that

$$e_1 f_1 + \cdots + e_n f_n = 0.$$

By injectivity, this means that

$$e_1 \otimes f_1 + \cdots + e_n \otimes f_n = 0.$$

Pick a k-basis β of F. Then the elements $e_i \otimes \beta_j$ are linearly independent, so it follows that each f_i is 0. This proves that $e_1, \dots, e_n$ are linearly independent over F. The other direction can be proved similarly by choosing bases. □

Proof of Theorem 7.2. $(1 \Rightarrow 4)$ Let's first assume that E/k is finite separable. Then $E = k(\alpha)$. Let f be the irreducible polynomial of α by the primitive element theorem. Then if $f = f_1 \dots f_n$ is the prime factorization of f,

$$E \otimes_k k' = k[x]/(f) \otimes_k k' = k'[x]/(f) = \prod_{i=1}^{n} \frac{k'[x]}{(f_i)}.$$

This is because f_i are distinct since f is separable and we can use the Chinese Remainder theorem. Hence this is isomorphic to a product of fields, which is obviously reduced.

$(4 \Rightarrow 3)$ Obvious since the latter is a special case of the former.

$(3 \Rightarrow 2)$ It suffices to show that E is linear disjoint from L for any $L \subset k^{\mathrm{perf}}$ and L/k is finite, say $L = k(\beta_1, \dots, \beta_n)$. Let's first treat the case when $n = 1$. Then the irreducible polynomial of β is of the form $x^{p^e} - a$ for some $a \in k$. Then

$$E \otimes_k L = \frac{L[x]}{(x^{p^e} - a)}.$$

This is either a field or non-reduced depending on whether $x^{p^e} - a$ is reducible in L or not (since the factorization is of the form $(x^{p^{e'}} - a')^{p^{e-e'}}$ for some $a' \in L$). The latter case cannot happen by our assumption, so the former holds, i.e., $E \otimes_k L$ is a field, and E and L are linearly disjoint. The general case can be handled similarly.

$(2 \Rightarrow 1)$ Assume in contrary that E/k is not separable. Then there exists an element $\alpha \in E$ such that α is not separable over k. Since $k(\alpha)$ is a subfield of E and E is linearly disjoint from k^{perf}, it follows that $k(\alpha)$ is also linearly disjoint from k^{perf}. Note that the irreducible polynomial of α can be written as $f(X^{p^e})$, where f is irreducible separable and $e > 0$. Let $\deg f = d$. Then $\deg \alpha = dp^e$. Now observe that $1, \alpha, \dots, \alpha^{dp^e - 1}$ are linearly independent over k. By our assumption, they are linearly independent over the perfect closure as well. However, if we write the irreducible polynomial of α as $x^{dp^e} + a_1 x^{(d-1)p^e} + \cdots + a_d$, then this is a power of the polynomial $g(x)^{p^e}$ with coefficients in k^{perf}. Hence the degree of α over k^{perf} is less than or equal to d, which is strictly less than dp^e. This is a contradiction! □

§ Lecture 8

Now we can talk about one of the main objects of study in this course.

Definition 8.1. Let A be a commutative k-algebra such that $\dim_k A$ is finite. We say that A is a *reduced k-algebra* if A is reduced as a ring. (i.e. A has no non-zero nilpotent elements). We say that A is an *etale k-algebra* if $A \otimes_k k'$ is reduced k'-algebra for any field extension k'/k.

Example 8.1.1. If E/k is a finite field extension, then of course E is reduced. Moreover, E is an etale k-algebra if and only if E is separable over k.

Fact 8.1. *If A_1 and A_2 are reduced (resp. etale) k-algebras, then $A_1 \times A_2$ is also reduced (resp. etale).*

Theorem 8.1. *Let A be a commutative k-algebra of finite degree. Then A is reduced iff $A \cong E_1 \times \cdots \times E_n$ where E_i are finite extensions of k.*

Proof. One direction follows readily from the observations that we made above. Now let's show another direction. It suffices to show that if A is reduced and not a field, then $A \cong A_1 \times A_2$ for two reduced algebras A_1 and A_2 which are non-zero.

In order to decompose a ring R into the product of two rings R_1 and R_2, we can start by finding a central idempotent e. Then $1-e$ is also a central idempotent, and we can map $a \mapsto ae + a(1-e)$ which is easily shown to give a ring isomorphism $R \to Re \times R(1-e)$. (This is kind of like finding an orthonormal basis and taking the dot products.)

Let I be a non-zero finitely generated proper ideal of A of minimal dimension. Now consider the ideal $I^2 \subseteq I$. This ideal is non-zero, because it must contain an element of the form a^2 where $a \in I$ is non-zero. Therefore, by the minimality of dimension of I, this forces $I^2 = I$. Now we can use a nice little lemma from commutative algebra.

Lemma 8.2. *Let A be a commutative ring, and I be a finitely generated ideal of A such that $I^2 = I$. Then I is principal and generated by an idempotent element.*

Proof. Suppose that I is generated by $u_1, \ldots, u_n$ over A. Then $I = I^2$ implies that $u_i \in I^2 = Iu_1 + \cdots + Iu_n$. This means that we can write

$$u_i = \sum_{i=1}^{n} a_{ji} u_j, \quad a_{ji} \in I.$$

Now let M be the matrix (a_{ij}). Then $I_n - M$ sends the vector $(u_1, \ldots, u_n)$ to 0. In particular, $\det(I_n - M)u_i = 0$ for all $i \leq n$. Note that this determinant is equal to $1 - e$ for some $e \in I$. Therefore, $eu_i = u_i$ for each i. Since they generate I, it follows that $eu = u$ for all $u \in I$, so in particular $e^2 = e$. Moreover, eA contains all u_i, so $eA \subseteq I \subseteq eA$. Thus, I is a principal ideal generated by e, and the lemma is proved. □

This finishes the proof of the theorem as well. □

Corollary 8.2.1. *Let $A = A_1 \times \cdots \times A_s$ be a reduced k-algebra, where each A_i is a finite field extension of k. Then A is an etale k-algebra if and only if each A_i is separable over k.*

Definition 8.2. Let A be a commutative algebra of finite dimension over k. We say that A is a split etale k-algebra if $A \cong k \times \cdots \times k$.

Lemma 8.3. *Let A be a commutative algebra of finite dimension over k. Then A is etale if and only if there exists a finite field extension k' of k such that $A \otimes_k k'$ is a split etale k'-algebra.*

Proof. We may assume that $A = E_1 \times E_2 \times \cdots E_s$ where E_i/k is a finite separable extension. It suffices to treat the case when $s = 1$. Assume that $E = E_1 = k[x]/(f)$ for some separable polynomial f, and let k' be a splitting field of f. Then

$$k[x]/(f) \otimes k' \cong k'[x]/(f) \cong \prod_{i=1}^{\deg f} k[x]/(x - \alpha_i) \cong \coprod_{i=1}^{\deg f} k$$

by the Chinese Remainder Theorem.

For the other direction, by Mac Lane's Theorem, it suffices to show that $A \otimes_k k^{\mathrm{perf}}$ is reduced. Note that

$$A \otimes_k (k')^{\mathrm{perf}} = (A \otimes_k k') \otimes_{k'} (k')^{\mathrm{perf}} = \prod_{i=1}^{n} k' \otimes_{k'} (k')^{\mathrm{perf}} = \coprod_{i=1}^{n} (k')^{\mathrm{perf}},$$

and so $A \otimes_k (k')^{\mathrm{perf}}$ is reduced. Since $A \otimes_k k^{\mathrm{perf}}$ is a subring of this ring, it follows that it is also reduced. Hence A is etale. □

§ Lecture 9

Theorem 9.1. *Suppose that A and A' are reduced, then so are $A \times A'$, any subalgebra of A and any quotient of A. If they are in addition etale, then the above three constructions and $A \otimes_k A'$ are all etale. Same goes for split etale algebras.*

Proof. The fact that the product preserves these is obvious. For the quotient, note that $A = k_1 \times \cdots \times k_s$ is a product of finite field extensions (resp. separable extensions). Any ideal of this ring is of the form $I_1 \times \cdots \times I_s$ where I_j are either the zero ideal or the whole ring, the quotient is still reduced (resp. etale). For the tensor product, use the previous proposition and note that the tensor product of split etale algebras are split etale. If A is etale and S is a subalgebra of A, then $S \otimes_k k' \subseteq A \otimes_k k'$ which is reduced, so S is also etale. □

Let k be a field. Then we can consider two categories, first the category of split etale k-algebras and the second the category of finite sets. Denote these by $\mathcal{C}$ and $\mathcal{D}$. Then we have

Theorem 9.2 (Toy version)**.** *$\mathcal{C}^{op}$ and $\mathcal{D}$ are equivalent.*

Proof. For any split etale A, we define $\mathbb{X}(A) = \mathrm{Hom}(A, k)$ and for any set X, we define $\mathbb{A}(X) = k^X$. We claim that these two functors are quasi-inverse to each other, so they give an equivalence between the two categories.

Note that $\mathbb{X} \circ \mathbb{A}$ maps a set X to $\mathrm{Hom}(k^X, k)$. For each element in $x \in X$, we can define a map $k^X \to k$ by evaluating at x (Here we are viewing k^X as functions from X to k.) In the other direction, for each element in $a \in A$, we can evaluate at a to get a map from $\mathrm{Hom}(A, k) \to k$, which is precisely an element of $k^{\mathrm{Hom}(A,k)}$. Denote these maps by t_X and r_A.

We claim that t_X and r_A are bijections for all X and for all A. This is just checking. □

Here is the main theorem that we are going to prove soon.

Theorem 9.3 (Grothendieck's Galois theory)**.** *Let k be a field. Fix a finite Galois extension $\overline{k}/k$. Put $G = \mathrm{Gal}(\overline{k}/k)$. Then the category of etale k-algebras that split after base change to $\overline{k}$ and the category of finite G-sets are contravariantly equivalent to each other. The correspondence is given by $A \mapsto \mathrm{Hom}(A, \overline{k})$ and $X \mapsto (\overline{k}^X)^G$ where the G-action on the latter set is $(g \circ \phi)(x) = g\phi(g^{-1}x)$.*

§ Lecture 10

Let k be a field, and let S be a set of monic, non-constant polynomials from $k[x]$.

Lemma 10.1. *If E_1 and E_2 are both splitting fields of S, then $E_1 \cong E_2$ as k-algebras.*

There is another variant of this lemma which is more enlightening to prove.

Lemma 10.2. *Let $\sigma : k_1 \to k_2$ be an isomorphism of fields. Let $S_1 \subseteq k_1[x]$ be a set of polynomials, and let $S_2 = \sigma(S_1)$. Assume that E_i/k_i is a splitting field of S_i. Then there exists an isomorphism $\overline{\sigma} : E_1 \to E_2$ extending σ.*

Proof. Let's first prove the case when $S_1 = \{f_1\}$. We will do induction on $\deg f_1$. If $\deg f_1 = 1$, it's obvious. When $\deg f_1 > 1$, pick a root α_1 of f_1 in E_1, and let g_1 be the irreducible polynomial of α_1 over k_1. Let $g_2 = \sigma(g_1)$. Then $g_2 \mid f_2$. Choose a root $\alpha_2 \in E_2$ of g_2. Then we see that there exists an isomorphism between $k_1(\alpha_1)$ and $k_2(\alpha_2)$, and this isomorphism extends σ. Now note that E_i is also a splitting field of $f_i(x)/(x - \alpha_i) \in k_i(\alpha_i)[x]$ over $k_i(\alpha_i)$, and we're done by induction.

When S is finite but has multiple elements, then the splitting field of S is the same as the splitting field of the polynomial which is the product of polynomials in S. Therefore, the above case applies and we're done.

The result is also valid for arbitrary S but we need to use transfinite induction. Write $S = \{f_i\}_{i \in I}$, where I is a well-ordered set. For $i \in I$, let $E_{s,i}$ to be the subfield of E_s generated by k_s and the roots of polynomials f_j where $j \leq i$. Suppose we have defined $\sigma_{i_0} : E_{1,i_0} \to E_{2,i_0}$. If i is a successor of i_0, then $E_{1,i}$ is a splitting field over E_{1,i_0} of f_i, so we can extend σ_{i_0} to $\sigma_i : E_{1,i} \to E_{2,i}$. In the case when i is a limit ordinal, then

$$E_{s,i} = \bigcup_{j<i} E_{s,j}.$$

Since we have defined σ_j's for all the subextensions $E_{s,j}$, and they're compatible with each other, it follows that we can define $\sigma_i : E_{1,i} \to E_{2,i}$ just by defining it elementwise. Hence we're done by transfinite induction. □

Lemma 10.3. *Let k be a field, and let E/k be an algebraic extension. Then TFAE:*

1. *E is algebraically closed.*
2. *E is a splitting field of the set of all monic polynomials of positive degree in $k[x]$.*

Proof. The fact that (1) ⇒ (2) is obvious. Now suppose that E is a splitting field of all monic polynomials of positive degree in k, and let E' be an algebraic extension of E. If $\alpha \in E'$, then α is algebraic over E and E is algebraic over k, so α is algebraic over k. Therefore, there exists an irreducible polynomial $f \in k[x]$ which has α as a root. Now note that f splits into linear factors in $E[x]$, so if α is a root of f, then it must be an element of E. This proves that $E' = E$, so E is algebraically closed as desired. □

Definition 10.1. A field extension $\overline{k}/k$ is called an *algebraic closure* of k, if $\overline{k}$ is algebraic over k, and it is algebraically closed.

Then the above lemma proves that

Corollary 10.3.1. *An algebraic closure of k exists, and any two algebraic closures of k are isomorphic as k-algebras.*

Definition 10.2. E is *separably closed* iff any separable extension of E is trivial.

Now we state an analogous statement.

Lemma 10.4. *Let k be a field, and let E/k be a separable extension. Then TFAE:*

1. *E is separably closed.*
2. *E is a splitting field of the set of all monic, separable polynomials of positive degree in $k[x]$.*

To prove this, we need a lemma which is an analgoue of the statement for algebraic extensions.

Lemma 10.5. *Let $E'/E/k$ be a tower of field extensions. Suppose that E'/E is separable and E/k is separable. Then E'/k is separable.*

Proof. We claim that $E \otimes_k k^{\text{perf}} \cong E^{\text{perf}}$. Once we prove this claim, then

$$E' \otimes_E E^{\text{perf}} = E' \otimes_E (E \otimes_k k^{\text{perf}}) = E' \otimes_k k^{\text{perf}}.$$

But the algebra on the left is reduced since E' is separable over E. Therefore, the algebra on the right is also reduced, and hence E' is separable over k.

We now prove the claim. Consider $\alpha \in E$, and let d be the degree of α over k^{perf}. Then the seemingly bigger extension $k^{\text{perf}}(\alpha^{1/p})/k^{\text{perf}}$ also has degree d. This is because if we write $f(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}$ to be the irreducible polynomial of α over k^{perf}, we can find elements $b_i \in k^{\text{perf}}$ such that $b_i^p = a_i$. Then if we define $g(x) = b_0 + b_1 x + \cdots + b_{d-1}x^{d-1}$, we see that

$$g(\alpha^{1/p})^p = \sum_{i=0}^{d-1} b_i^p \alpha^i = \sum_{i=0}^{d-1} a_i \alpha^i = f(\alpha) = 0,$$

so g is a polynomial of degree d having $\alpha^{1/p}$ as a root. Therefore, $k^{\text{perf}}(\alpha^{1/p}) = k^{\text{perf}}(\alpha)$, so $\alpha^{1/p} \in k^{\text{perf}}(\alpha) \subseteq Ek^{\text{perf}}$. This shows that $\alpha^{\frac{1}{p^n}} \in Ek^{\text{perf}}$, so we must have $E^{\text{perf}} \subseteq Ek^{\text{perf}}$. Meanwhile, all the elements of Ek^{perf} belong to E^{perf} since all such elements are rational functions of a finite number of elements of E and k^{perf}, and we can choose a sufficiently large power of p to bring those elements in k^{perf} into k. Therefore, $Ek^{\text{perf}} = E^{\text{perf}}$. Finally we use the separability condition: since E is separable over k the surjection $E \otimes_k k^{\text{perf}} \to Ek^{\text{perf}}$ is an isomorphism and we're done. □

We will now prove the primitive element theorem which is very handy when dealing with finite separable extensions. Before this, we need a lemma.

Lemma 10.6. *Let E/k be a finite field extension, and suppose that there are only finitely many fields M such that $k \subseteq M \subseteq E$. Then E/k is simple.*

Proof. The result is obvious when k is finite, since every finite extension of a finite field is simple. Now assume that k is infinite. We write $E = k(\alpha_1, \ldots, \alpha_n)$, and we induct on n. When $n > 1$, by induction hypothesis, $k(\alpha_1, \ldots, \alpha_{n-1})$ is simple, so it is generated by some θ'. Now consider $k(\theta' + c\alpha_n)$, where $c \in k$. This gives an infinite family of field extensions lying between E and k, so by the assumption, this gives two distinct elements c and c' such that $k(\theta' + c\alpha_n) = k(\theta' + c'\alpha_n)$. Then this extension contains both θ and α_n, so it must contain E, and hence equal to E. This proves that E/k is simple as desired. □

Corollary 10.6.1 (Primitive element theorem). *Let E/k be a finite, separable extension. Then E/k is simple.*

Proof. By the above lemma, we just need to show that there are only finitely many fields between E and k. Let k' be an extension of k such that $E \otimes_k k'$ is a split etale k'-algebra. Given any intermediate field M, we can form a k'-subalgebra of $E \otimes_k k'$ just by tensoring with k'. This map is injective, but the set of k'-subalgebras of $E \otimes_k k'$ is finite. Therefore, we're done. □

Theorem 10.7. *Let E/k be an algebraic extension. TFAE:*

1. *E is a splitting field of S for some $S \subseteq k[x]$.*
2. *For any algebraic closures $\overline{k}/k$ and any k-algebra homomorphisms $\sigma, \sigma' : E \to \overline{k}$, the images are the same.*
3. *For any irreducible $f \in k[x]$, if f has a root in E, then f splits completely in $E[x]$.*

Proof. (1) $\Rightarrow$ (2): Let T be the set of roots of polynomials in S in E. Then by definition, $E = k(T)$. Then $\sigma(E) = k(\sigma(T))$ and $\sigma(E') = k(\sigma'(T))$. But note that the definition of $\sigma(T)$ and $\sigma'(T)$ are completely independent of σ and σ' (they are just the elements of $\overline{k}$ which are the roots of the polynomials in S). Therefore, $\sigma(T) = \sigma'(T)$ and we're done.

(2) $\Rightarrow$ (3): Suppose that f is an irreducible polynomial in $k[x]$. WLOG, assume that E is contained in a fixed algebraic closure $\overline{k}$, let α be a root of $f \in E$, and let α' be any other root of f in $\overline{k}$. Then we can construct a homomorphism $k(\alpha) \to \overline{k}$ which maps α to α', and this homomorphism can be extended to get a homomorphism $E \to \overline{k}$. However, we know that the image of this homomorphism must be E itself. Therefore, $\alpha' \in E$, and it follows that f splits in $E[x]$.

(3) $\Rightarrow$ (1): Take a subset $T \subset E$ such that $E = k(T)$. Let S be the set of irreducible polynomials of elements in T. Then each polynomial in S splits in E by our assumption, and the roots of polynomials in S contain T so they certainly generate E. Therefore, E is the splitting field of S over k. □

Definition 10.3. If E/k satisfies these equivalent conditions, we say E/k is a *normal* extension.

Definition 10.4. An algebraic extension E/k is *Galois* if the extension is both separable and normal.

Definition 10.5. The *Galois group* of a Galois extension E/k is the set of automorphisms of E which fix k.

It turns out that this group has more structure than just being a group. As a start, we will put a topology on G. Let E^E be the set of maps from $E \to E$. Then this set can be thought of as $\prod_{i \in E} E$. We can then give each copy of E the discrete topology, and give the set E^E the product topology. Now since G is a subset of E^E, we can endow G with the subspace topology.

§ Lecture 11

In the following, we denote the separable closure of a field k by k^{sep}.

We're now in a position to prove Theorem 9.3.[1] Let k be a field, and let $\overline{k}$ be a finite Galois extension of k with Galois group G. We want to prove that there is an anti-equivalence between the category of etale k-algebras A such that $A \otimes_k \overline{k}$ is a split etale $\overline{k}$-algebra, and the category of finite G-sets. The equivalence functors are given by

$$\mathbb{X} : A \mapsto \text{Hom}_k(A, \overline{k}) \quad \text{and} \quad \mathbb{A} : X \mapsto (\overline{k}^X)^G$$

Here, the G-action on $\overline{k}^X$ is given by $(g \cdot f)(x) = g(f(g^{-1} \cdot x))$. This condition is equivalent to the fact that f is a G-set homomorphism from X to $\overline{k}$ (Remember that the underlying set of $\overline{k}$ has a G-set structure almost by definition.) To see this, if we replace $g^{-1} \cdot x$ by y, then $f \in (\overline{k}^X)^G$ iff

$$(g \cdot f)(x) = f(x) \quad \forall x \in X, \forall g \in G \iff f(g \cdot y) = g(f(y)) \quad \forall y \in X, \forall g \in G.$$

Therefore, $\mathbb{A}(X) = \text{Hom}_{G\text{-}\mathsf{Set}}(X, \overline{k})$.

Below are some properties of this equivalence that will be useful for later.

(1) If A corresponds to X, then $\dim_k A = |X|$.

(2) $\mathbb{X}$ and $\mathbb{A}$ invert categorical constructions. In particular, if A_1 is an etale algebra which corresponds to the G-set X_1 and A_2 corresponds to X_2, then $A_1 \times A_2$ corresponds to $X_1 \sqcup X_2$.

We will prove the second property first.

Proof. Let A be an etale k-algebra, and let $A = F_1 \times F_2 \times \cdots \times F_n$ be its representation as a product of separable field extensions of k. If $\phi : A \to \overline{k}$ is a homomorphism, then the kernel of this map must be a prime ideal, which can only be of the form $F_1 \times \cdots \times F_{i-1} \times F_{i+1} \times \cdots \times F_n$ for some i. Consequently, ϕ is composed of a projection onto F_i followed by a homomorphism from F_i to $\overline{k}$. Therefore, it follows that

$$\text{Hom}_k(A, \overline{k}) = \bigsqcup_{i=1}^{n} \text{Hom}_k(F_i, \overline{k}).$$

From this, it is obvious that if A_1 and A_2 are two etale algebras, then $\text{Hom}_k(A_1 \times A_2, \overline{k}) = \text{Hom}_k(A_1, \overline{k}) \sqcup \text{Hom}_k(A_2, \overline{k})$.

Now let X be a G-set, and let $X = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_n$ be its decomposition into orbits. Pick an orbit X_i, and let x_i be an element in the orbit. Then any G-set homomorphism from X_i to $\overline{k}$ is determined by the image of the element x. This image can be any element in the subfield of $\overline{k}$ fixed by the stabilizer of x_i. Therefore,

$$\text{Hom}_{G\text{-}\mathsf{Set}}(X, \overline{k}) = \prod_{i=1}^{n} \text{Hom}_{G\text{-}\mathsf{Set}}(X_i, \overline{k}) = \prod_{i=1}^{n} k^{\text{Stab}(x_i)}.$$

From this, it is obvious that if X_1 and X_2 are two G-sets, then

$$\text{Hom}_{G\text{-}\mathsf{Set}}(X_1 \sqcup X_2, \overline{k}) = \text{Hom}_{G\text{-}\mathsf{Set}}(X_1, \overline{k}) \times \text{Hom}_{G\text{-}\mathsf{Set}}(X_2, \overline{k}). \qquad \square$$

The first property is just a corollary of this.

[1] For a proof of this theorem in the case when the extension is the separable closure of k, see Theorem 2.9 in https://websites.math.leidenuniv.nl/algebra/GSchemes.pdf

Corollary 11.0.1. $\dim_k A = |\mathrm{Hom}_k(A, \overline{k})|$ *for any k-algebra A such that $A \otimes_k \overline{k}$ is a split $\overline{k}$-algebra.*

Proof. Note that if A splits over $\overline{k}$, then all the F_i also split over $\overline{k}$. Since F_i are separable, this means that $|\mathrm{Hom}_k(F_i, \overline{k})| = \dim_k F_i$. Since $\dim_k A = \sum_{i=1}^n \dim_k F_i$, the result follows. □

Remark. Actually, we can prove a stronger proposition. Let A be a d-dimensional k-algebra. Then for any field extension $\overline{k}/k$, $|\mathrm{Hom}_k(A, \overline{k})| \leq d$ with equality if and only if A is etale. If $A' = A \otimes \overline{k}$ is not reduced, then we can consider the nilradical I. I is contained in the kernel of any homomorphism from A' to $\overline{k}$, and A'/I is reduced, so

$$\mathrm{Hom}_k(A, \overline{k}) = \mathrm{Hom}_{\overline{k}}(A', \overline{k}) = \mathrm{Hom}_{\overline{k}}(A'/I, \overline{k}) = \dim_{\overline{k}}(A'/I) \leq d.$$

Corollary 11.0.2. $|\dim_k(\overline{k}^X)^G| = |X|$.

Proof. If this is true for $X = X_1$ and X_2, then it is also true for $X_1 \sqcup X_2$. Therefore, we may assume that X is a single orbit $= G/H$. Again, as k-algebras,

$$(\overline{k}^X)^G = \mathrm{Hom}_{G\text{-}\mathsf{Set}}(X, \overline{k}) = \mathrm{Hom}_{G\text{-}\mathsf{Set}}(G/H, \overline{k}) \cong \overline{k}^H.$$

Hence what we're trying to show is just that $\dim_k(\overline{k}^H) = |G/H|$. This follows from classical Galois theory, but we can also use the following theorem by Artin. □

Theorem 11.1 (Artin)**.** *Let E be a field, and let H be a finite subgroup of* $\mathrm{Aut}(E)$*. Put $k = E^H$. Then E/k is Galois of degree $|H|$ with Galois group H.*

Proof. Let $\alpha \in E$, and let

$$f(x) = \prod_{\sigma \in H'} (x - \sigma(\alpha)).$$

where H' is the quotient of H by the stabilizer of $\alpha \in H$. Then the coefficients of this polynomial are fixed by H, so they belong to k. This shows that α has degree at most $|H|$. Moreover, α is separable since f has distinct roots and the minimal polynomial of α must divide f.

We now claim that E/k is finite of degree at most $|H|$. Take $\alpha \in E$ such that $[k(\alpha) : k]$ is maximum. If $k(\alpha)$ is not the whole field E, then there exists an element β outside of $k(\alpha)$. Then the field extension $k(\alpha, \beta)$ is strictly bigger than $k(\alpha)$, and since this is a finite separable extension, this implies that there exists a γ that generates this extension; this γ then has bigger degree than α which is a contradiction.

Now note that given any homomorphism from $E \to \overline{k}$, we can compose it with an element of H to get another homomorphism from $E \to \overline{k}$. Since E/k is separable,

$$[E : k] = [E : k]_s \coloneqq |\mathrm{Hom}_k(E, \overline{k})| = |H||\text{number of distinct images of } E \text{ in } \overline{k}|.$$

This proves that $[E : k] = |H|$, and that E has fixed image in $\overline{k}$, so E is a normal extension of k. Hence E is Galois, and the Galois group of E is precisely H. □

[*Scribbling my own thoughts...*]

Here is a version of Grothendieck's Galois theory when the field extension is not necessarily finite (we are looking at $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ which is really big.) In this case, we have to consider the Krull topology on the Galois group to maintain the Galois correspondence. The following notes are taken from Szamuely's *Galois Groups and fundamental Groups*. These were written way before I revised this part, so a lot of the steps are redundant. They are not part of the lectures, and there may be some errors.

Theorem 11.2. *Let k be a field, and fix a separable closure k_s of k. Let $\mathrm{Gal}(k) = \mathrm{Gal}(k_s/k)$. Then the functor mapping a finite etale k-algebra A to the finite set $\mathrm{Hom}_k(A, k_s)$ gives an anti-equivalence between the category of finite etale k-algebras, and the category of finite sets with continuous left $\mathrm{Gal}(k)$-action. Here, separable field extensions give rise to sets with transitive $\mathrm{Gal}(k)$-action, and Galois extensions to $\mathrm{Gal}(k)$-sets isomorphic to finite quotients of $\mathrm{Gal}(k)$.*

Before proving this, we will prove the special case for finite separable extensions. The statement goes as follows:

Theorem 11.3. *Let k be a field with a fixed separable closure k_s. The contravariant functor mapping a finite separable extension L/k to the finite $\mathrm{Gal}(k)$-set $\mathrm{Hom}_k(L, k_s)$ gives an anti-equivalence between the category of finite separable extensions of k and the category of finite sets with continuous and transitive $\mathrm{Gal}(k)$-action. Here, Galois extensions give rise to $\mathrm{Gal}(k)$-sets isomorphic to some finite quotient of $\mathrm{Gal}(k)$.*

Proof. Let L/k be a finite separable extension. Then the $\mathrm{Gal}(k)$-action on $\mathrm{Hom}_k(L, k_s)$ is given by $g \cdot \phi = g \circ \phi$.

Claim 1. This action is continuous.

Proof of Claim 1. Recall that the G-action on a finite set X with discrete topology is continuous iff the stablizer of any element $x \in X$ is open in G. To see this, pick any element $x \in X$. Then the preimage of x under the map is the set of tuples (g, y) such that $gy = x$. This can be written as a union

$$\bigcup_{y \in G} \{(g, y) \mid gy = x\} = \bigcup_{y \in G} G_y.$$

If y is not in the same orbit as x, then G_y is the empty set. If y is in the same orbit, then $G_y = \mathrm{Stab}(x)g$ for any $g \in G_y$. Since right multiplication by g is a homeomorphism, G_y is open if $\mathrm{Stab}(x)$ is open in G. Conversely, if the G-action is continuous, then the map $G \to X$ defined by $g \mapsto (g, x) \mapsto gx$ is continuous. Now observe that $\mathrm{Stab}(x)$ is the preimage of x under this map, and since X has the discrete topology, $\mathrm{Stab}(x)$ must be open.

Now let's apply this to our case. Take any embedding $i : L \to k_s$ which fixes k, and let U be the stabilizer subgroup of i under the $\mathrm{Gal}(k)$-action. Then U is precisely the elements of $\mathrm{Gal}(k)$ which fix the image of L under i. Equivalently, we have $U = \mathrm{Gal}(k_s/i(L))$. Since $\dim L/k$ is finite, U is closed with finite index in $\mathrm{Gal}(k)$ due to Galois correspondence. Hence it is open and we're done. □

This action is also transitive on $\mathrm{Hom}_k(L, k_s)$. By the primitive element theorem, $L = k(\theta)$ for some θ. Let f be the minimal polynomial of θ over k. Then each homomorphism in $\mathrm{Hom}_k(L, k_s)$ corresponds to a root of f in k_s, and for any two roots in k_s there exists an automorphism of k_s/k mapping one to the other. Therefore, we have proven that this functor is at least well-defined on the objects. Regarding the maps, it is easy to show that if L and M are finite separable extensions of k and $f : L \to M$ is a homomorphism fixing k, then $f^* : \mathrm{Hom}_k(M, k_s) \to \mathrm{Hom}_k(L, k_s)$ defined by $\phi \mapsto \phi \circ f$ is a $\mathrm{Gal}(k)$-set homomorphism.

Claim 2. This functor is essentially surjective.

Proof of Claim 2. Let X be a finite set with continuous, transitive $\mathrm{Gal}(k)$-action. Take any element s. Then the stabilizer $U = \mathrm{Stab}(s) \subseteq \mathrm{Gal}(k)$ is open, so it is a closed subgroup of finite index. Therefore, by Galois correspondence, we can consider the fixed field $L = k_s^U$. We now claim that $\mathrm{Hom}_k(L, k_s) \cong X$ as $\mathrm{Gal}(k)$-sets. Note that X is isomorphic to the space of left cosets of U in

$\mathrm{Gal}(k)$ under left multiplication (The isomorphism is given by mapping any element y to the coset gU where g is any element of $\mathrm{Gal}(k)$ such that $gs = y$.) However, also note that $\mathrm{Hom}_k(L, k_s)$ is also isomorphic to this set. The elements of U are precisely the ones that fix the natural inclusion $i : L \to K_s$, and we can safely map the embedding $g \circ i$ to the coset gU. □

Claim 3. This functor is fully faithful.

Proof of Claim 3. Let M and L be finite separable extensions of k. Then we have to show that this functor induces a bijection between the following two sets

$$\{\text{maps from } L \text{ to } M\} \iff \{\text{maps from } \mathrm{Hom}_k(M, k_s) \text{ to } \mathrm{Hom}_k(L, k_s)\}.$$

Fix any element $\phi \in \mathrm{Hom}_k(M, k_s)$. Since $\mathrm{Hom}_k(M, k_s)$ is a transitive $\mathrm{Gal}(k)$-set, any map from $\mathrm{Hom}_k(M, k_s)$ to $\mathrm{Hom}_k(L, k_s)$ is completely determined by its image of ϕ. Take any such map f. Since f is a $\mathrm{Gal}(k)$-set homomorphism, the stabilizer of ϕ must also fix the stabilizer of $f(\phi)$, so $U = \mathrm{Stab}(\phi) \subseteq \mathrm{Stab}(f(\phi)) = V$. Via the Galois correspondence, this gives us two subfields M' and L' fixed by U and V respectively, and we see that $L' \subseteq M'$ and that $L' = f(\phi)(L)$ and $M' = \phi(M)$. If we denote $\psi : \phi(M) \to M$ be the inverse isomorphism, then $\psi \circ f(\phi)$ is the unique homomorphism in $\mathrm{Hom}_k(L, M)$ that induces f as desired. □

Combining all of this establishes an equivalence between the two categories. Note that when L/k is Galois, the stabilizer subgroup is normal, so the space of left cosets is actually isomorphic to the quotient of the Galois group by the stabilizer. This completes the proof. □

Now we are ready to provide a proof of Theorem 11.3.

Proof of Theorem 11.3. Let A be a finite etale k-algebra, and write A as a product $L_1 \times L_2 \times \cdots \times L_n$ which are finite separable extensions of k.

Claim 1. Any k-algebra homomorphism in $\mathrm{Hom}_k(A, k_s)$ can be factored as a projection onto one of the L_i followed by an embedding in $\mathrm{Hom}_k(L_i, k_s)$.

Proof of Claim 1. Note that the kernel of any homomorphism in $\mathrm{Hom}_k(A, k_s)$ must be a prime ideal, hence it can only be of the form $L_1 \times \cdots \times \{0\} \times \cdots \times L_n$. Therefore, the image is isomorphic to one of the L_i, and by the universal property of quotients, we can find a unique map from $L_i \to k_s$ such that our desired property holds. □

This claim shows that $\mathrm{Hom}_k(A, k_s)$ can in fact be realized as the disjoint union of $\mathrm{Hom}_k(L_i, k_s)$, and since the $\mathrm{Gal}(k)$-action on these sets is transitive, this is in fact the orbit decomposition of $\mathrm{Hom}_k(A, k_s)$. This lets us prove essential surjectivity: given a finite set X with continuous $\mathrm{Gal}(k)$-action, we can decompose it into its orbits, and then construct a finite separable extension L_i for each orbit, and finally take their product to get the desired etale k-algebra.

Similarly, a map between etale k-algebra $A = \prod_i L_i$ and $A' = \prod_j L'_j$ is a collection of maps from some L_i to each L'_j for all j. For each of these maps, we get a unique map $\mathrm{Hom}_k(L'_j, k_s) \to \mathrm{Hom}_k(L_i, k_s)$. Finally, we get a map from the disjoint union $\mathrm{Hom}_k(A', k_s) \to \mathrm{Hom}_k(A, k_s)$. This argument shows that the functor is fully faithful. □

[*Scribbling ends*]

§ Lecture 12

We recall the fundamental theorem:

Theorem 12.1. *Let $\overline{k}/k$ be a finite Galois extension of fields, and let $G = \mathrm{Gal}(\overline{k}/k)$. Then let Et_k be the category of etale k-algebras k such that $A \otimes_k \overline{k}$ is a split-etale $\overline{k}$-algebra. Let G-Set be the category of finite G-sets with continuous G-action. Then Et_k and G-Set are anti-equivalent. The functors are given by $\mathbb{X}(A) = \mathrm{Hom}_k(A, \overline{k})$ and $\mathbb{A}(X) = (\overline{k}^X)^G$.*

Proof. We have to show two natural isomorphisms: first, that

$$A \cong (\overline{k}^{\mathrm{Hom}(A,\overline{k})})^G,$$

and that

$$X \cong \mathrm{Hom}_k((\overline{k}^X)^G, \overline{k}).$$

We have already shown before that

$$\dim_k A = |\mathrm{Hom}_k(A, \overline{k})| \quad \text{and} \quad |X| = \dim(\overline{k}^X)^G.$$

To prove the first bijection, we may assume that A is a separable field extension of k. Let the evaluation map from $A \to (\overline{k}^{\mathrm{Hom}(A,\overline{k})})^G$ be ϕ. Then ϕ is non-zero and hence injective. Since these k-algebras both have the same dimension over k, it follows that ϕ is an isomorphism. The general case follows from writing A as a product of separable extensions.

To prove the second bijection, let ψ be the map under consideration. Note that both the left hand side and right hand side have the same size, so we just need to show that ψ is injective. Therefore, take $x, x' \in X$. Then we need to find some $f \in (\overline{k}^X)^G$ such that $f(x) \neq f(x')$. If x, x' are not in the same G-orbit, then we can take $f(y) = 1$ if y is in the G-orbit of x, and 0 otherwise. This function is evidently invariant under the Galois group, so it belongs to $(\overline{k}^X)^G$, and satisfies $f(x) = 1$ and $f(x') = 0$. Therefore, assume that $x' = gx$ for some x.

Consider the set of functions $f \in (\overline{k}^X)^G$ such that $f = 0$ outside the G-orbit of x. This orbit is isomorphic to the coset G/H where $H = \mathrm{Stab}_G(x)$. Therefore, we can identify this set with the set $\overline{k}^H$. If an element g' fixes $\overline{k}^H$, then $g' \in \mathrm{Gal}(\overline{k}/\overline{k}^H) = H$, so as $g \notin H$, we can find some $a \in \overline{k}^H$ such that $a \neq ga$. Let $f(x)$ be such that $f(x) = a$. Then $f(x') = f(gx) = ga \implies f(x) \neq f(x')$. □

We now show that Grothendieck's formulation implies the classical fundamental theorem of Galois theory.

Theorem 12.2. *Suppose that we have a finite Galois extension $\overline{k}/k$ with Galois group G. Then there exists an inclusion-reversing bijection between subgroups of G and intermediate fields F such that $k \subseteq F \subseteq \overline{k}$. The correspondence is given as follows: given a field F, we can take its automorphism group $\mathrm{Gal}(\overline{k}/F)$, and given any subgroup H, we can take its fixed field $\overline{k}^H$.*

Proof. Our first goal is to convert this into categorical language. We can view the subgroups of G as subobjects of the G-set $G/\{1\}$ in the opposite category of G-Set. On the other hand, k-subfields of $\overline{k}$ are subobjects of $\overline{k}$ in the category of etale k-algebras that split over $\overline{k}$. These are in bijection by Grothendieck's formulation. □

Corollary 12.2.1. *Under this correspondence, F/k is Galois iff $H \trianglelefteq G$.*

Proof. F/k is Galois iff $|\mathrm{Aut}_{G\text{-}\mathsf{Set}}(G/H)| = [G : H]$. However, note that $\mathrm{Aut}_{G\text{-}\mathsf{Set}}(G/H) = N_G(H)/H$. Therefore, this implies that $N_G(H) = G$, which means that H is normal in G. □

Theorem 12.3 (Normal basis theorem). *Let E/k be a finite Galois extension of fields. Let $G = \mathrm{Gal}(E/k)$. Then there exists $a \in E$ such that $\{ga\}_{g\in G}$ is a basis of the k-vector space E. In other words, E as a $k[G]$-module is free of rank n.*

One way to solve such a problem is to generalize the statement into that of an etale algebra. Therefore, we want to define what we mean by an etale k-algebra to be Galois. Obviously, our definition should cover all the Galois extensions of fields E/k, and it should also be stable under base change; $E \otimes_k k'$ should be Galois over k'. Therefore, we define

Definition 12.1. Let G be a finite group, and k be a field. A *Galois G-algebra* over k is a pair (A, α) such that

1. A is an etale k-algebra,
2. α is a group homomorphism from G to $\mathrm{Aut}_k(A)$,
3. $|G| = \dim_k A$, and
4. $A^G = k$.

As usual, suppose that $\overline{k}/k$ is a finite Galois extension such that $A \otimes_k \overline{k}$ is split, and let $\Gamma = \mathrm{Gal}(\overline{k}/k)$. We want to investigate the properties of the Γ-set $X = \mathrm{Hom}_k(A, \overline{k})$ corresponding to A. This set also has many properties:

1. X is a finite Γ-set,
2. G acts on X by Γ-set automorphisms on the right,
3. $|G| = |X|$,
4. X_G is a singleton, i.e., the G-action is transitive.[2]

More explicitly, if $\sigma = \alpha(g)$ is an automorphism of A, then the action of g on $X = \mathrm{Hom}_k(A, \overline{k})$ is defined by $\phi \cdot g = \phi \circ \sigma$. The reason why this is a right action is because we have an *anti-equivalence* instead of an equivalence between Et_k and Set.

Remark. We often think of X as a set in which Γ acts on the left and G acts on the right, such that $(\gamma x)g = \gamma(xg)$. The last two conditions imply that X is a principal homogeneous space of G as a G-set.

We can now state the generalized version of the normal basis theorem.

Theorem 12.4. *Let (A, α) be a Galois G-algebra. Then there exists $a \in A$ such that $\{ga\}_{g\in G}$ is a basis of the k-vector space A.*

We will first prove this when k is infinite.

[2] Proof can be found in Prop. 18.14 in "The Book of Involutions" by Merkurjev, Tignol and Knus.

Proof. Observe that if A is split, then the theorem is true. If we write $A = k^X$, viewing elements of A as tuples indexed over the set X, then we see that $\mathrm{Hom}_k(A, \overline{k}) \cong X$ as sets; each homomorphism is just a projection onto the x-th coordinate for each $x \in X$. However, the first set has a right G-action, so we can transfer this action to the set X itself; if f is projection onto the x-th coordinate, then $f \cdot g$ is the projection onto the $x \cdot g$-th coordinate. In particular, if we fix an x_0 and denote by δ_{x_0} the tuple whose value is 1 at x_0 and 0 otherwise, then we see that the x-th coordinate of $g\delta_{x_0}$ is the same as $x \cdot g$-th coordinate of δ_{x_0}. Since X is a principal homogenous space of G, for any $x \in X$ we can find a unique g such that $x \cdot g = x_0$. Then we see that $g\delta_{x_0}$ is a tuple which is 1 at x-th coordinate and 0 otherwise. Therefore, $\{g\delta_{x_0}\}_{g \in G}$ is just the standard basis of k^X.

For the general case, we want to base change to a bigger field such that the algebra becomes split, and use the above case. But first, we need to know when $a \in A$, where A is split, gives a normal basis $\{ga\}_{g \in G}$. It is easy to see that this is the case when the matrix $(\sigma(ga))_{g \in G, \sigma \in \mathrm{Hom}_k(A,k)}$ is non-singular (by the above, all the elements in $\mathrm{Hom}_k(A, k)$ are projections.) In fact, this holds even when A is not split. The proof is by a base change argument. Let k'/k be such that $A' \coloneqq A \otimes_k k'$ is a split k'-algebra. Then A' is also a Galois G-algebra with G-action given by $g(a \otimes b) = ga \otimes b$. Now note that $\{ga\}_{g \in G}$ is a k-basis of A iff $\{ga \otimes 1\}_{g \in G}$ is a k'-basis of $A \otimes_k k'$. Moreover, we also have $\mathrm{Hom}_k(A, k) = \mathrm{Hom}_{k'}(A', k')$, so it turns out that the matrices $(\sigma(ga))_{g \in G, \sigma \in \mathrm{Hom}_k(A,k)}$ and $(\sigma(ga \otimes 1))_{g \in G, \sigma \in \mathrm{Hom}_{k'}(A',k')}$ are the same. Therefore, the former is invertible iff the latter is, and this proves the claim.

Let $v_1, \ldots, v_n$ be a basis of A over k. Then $a = \sum c_i v_i$ gives rise to a normal basis iff $(\sigma(ga))_{g \in G, \sigma \in \mathrm{Hom}(A,k)}$ is non-singular. Call this matrix $M(a)$. This matrix is non-singular iff $\det(M(a))$ is non-zero, which is a polynomial in $c_1, \ldots, c_n$ with coefficients in k, say F. The normal basis theorem in the split case then implies that there exists $c_1, \ldots, c_n \in k'$ such that $F(c_1, \ldots, c_n) \neq 0$. Assuming our field k is infinite, this implies that there exists $c_1, \ldots, c_n \in k$ such that $F(c_1, \ldots, c_n) \neq 0$ (otherwise it'd be the zero polynomial.) $\square$

§ Lecture 13

We continue to prove the normal basis theorem in the case when k is a finite field. For simplicity, assume that A is a field. Such an extension is necessarily cyclic by finite field theory.

Lemma 13.1. *Let A/k be a finite Galois extension such that $\mathrm{Gal}(A/k)$ is cyclic of order n. Let σ be a generator. Then there exists an element $\alpha \in A$ such that $\{\sigma^i \alpha\}$ is a basis of A.*

Proof. Note that we can view A as a $k[x]$-module by mapping x to σ. Then by the fundamental theorem for finitely generated modules over a PID, we see that this module is isomorphic to

$$\frac{k[x]}{(f_1)} \oplus \cdots \oplus \frac{k[x]}{(f_s)},$$

where $f_1 \mid f_2 \cdots \mid f_s \mid x^n - 1$. Now assume that $s \geq 2$. Then $\deg f_s < n$, and the module is killed by f_s. This means that if we write $f_s = c_0 + c_1 x + \cdots + c_d x^d$, then

$$c_0 + c_1 \sigma(a) + c_2 \sigma^2(a) + \cdots + \sigma^d(a) = 0$$

for all $a \in A$. However, a result of Dedekind shows that $\mathrm{id}, \sigma, \ldots, \sigma^{n-1}$ are linearly independent. This implies that $s = 1$, so $\deg f_s = n$, and hence $f_s = x^n - 1$. Therefore, A is isomorphic to $k[x]/(x^n - 1)$ as $k[x]$-modules. If we denote the image of x by α in this isomorphism, then α satisfies the property that we desire. □

Recall the definition of a Galois G-algebra A and its corresponding G-set $X \coloneqq \mathrm{Hom}(A, \overline{k})$. Let $\overline{k}$ be a finite Galois extension of k such that $A \otimes_k \overline{k}$ is split etale, and let Γ be the Galois group $\mathrm{Gal}(\overline{k}, k)$.

Lemma 13.2. *We have a natural bijection between Galois G-algebras over k that split over $\overline{k}$ and group homomorphisms from Γ to G up to conjugation by G. The latter is in bijection with Γ-actions on a G-principal homogeneous space.*

Proof. We first prove the second statement. Fix a G-principal homogeneous space X. Then a Γ-action on X is just a group homomorphism $\Gamma \to \mathrm{Aut}_{G\text{-}\mathsf{Set}}(X)$. However, the latter is isomorphic to G, since once we fix a point $x_0 \in X$, any G-set automorphism of x_0 is determined by the image of x_0. This gives us a group homomorphism from $\Gamma \to G$. However, different choices of the base point x_0 can give different homomorphisms, and each of them are conjugates of each other. This shows that Γ-actions on X are in bijective correspondence with conjugacy classes of group homomorphisms from Γ to G.

The first statement now follows from the above; any Γ-action on a G-PHS X corresponds to a Galois G-algebra over k that splits over $\overline{k}$ according to the discussion after Definition 12.1. □

As a corollary of this, we obtain

Corollary 13.2.1. *If G is abelian, then Galois G-algebras over k that split over $\overline{k}$ are in correspondence with group homomorphisms from Γ to G.*

We illustrate the power of the principle above by some examples.

Fact 13.1. *Assume that k is a field. Let*

$$\mu_n(k) = \{a \in k^\times \mid a^n = 1\},$$

be the n-th roots of unity in k, and suppose that $|\mu_n(k)| = n$. Then for any $a \in k^\times$, $k(a^{\frac{1}{n}})/k$ is Galois with Galois group a subgroup of $\mu_n(k)$.

Proof. Let $F = k(a^{\frac{1}{n}})$. Then F/k is the splitting field of $x^n - a$, which is also separable; hence it is Galois. Therefore, $\mathrm{Gal}(F/k)$ acts on the set X of roots of $x^n - a$. However, note that X is also a $\mu_n(k)$-PHS, and the two actions commute since $\mu_n(k) \in k^\times$. This shows that there is a canonical homomorphism which embeds $\mathrm{Gal}(F/k)$ in $\mu_n(k)$. □

Fact 13.2. *Let* $\mathrm{char}(k) = p > 0$*, and for any* $a \in k$*, let* α *be a root of* $x^p - x - a$*. Then* $k(\alpha)/k$ *is Galois with Galois group a subgroup of* $(\mathbb{F}_p, +)$*.*

Proof. Note that if α is a root of $x^p - x - a$, then the other roots are exactly $\alpha+1, \alpha+2, \ldots, \alpha+p-1$. Hence $k(\alpha)$ is normal over k, and α is of course separable over k so this is a Galois extension. Now note that the action of the Galois group commutes with the action of $(\mathbb{F}_p, +)$ on the set of these roots which we call X. Therefore, there exists an embedding of $\mathrm{Gal}(F/k)$ inside $\mathrm{Aut}_{\mathbb{F}_p\text{-}\mathsf{Set}}(X) = (\mathbb{F}_p, +)$. □

Fact 13.3. *Let* k *be a field such that* $n \neq 0$ *in* k*, and let* $k(\mu_n)$ *be the splitting field of* $x^n - 1$ *over* k*. Then this extension is Galois and its Galois group embeds into* $(\mathbb{Z}/n\mathbb{Z})^\times$ *canonically.*

Proof. Let X be the set of generators of μ_n. Then $\mathrm{Gal}(k(\mu_n)/k)$ acts faithfully on X. In fact, note that for any cyclic group C of order n, the set of generators of C is a PHS of $\mathrm{Aut}(C) = (\mathbb{Z}/n\mathbb{Z})^\times$. By the boilerplate above, we see that $\mathrm{Gal}(k(\mu_n)/k)$ embeds into $(\mathbb{Z}/n\mathbb{Z})^\times$. □

In fact, we can even prove the classic theorem on solvability by radicals.

Theorem 13.3. *If* $f(x) \in k[x]$ *has roots solvable by radicals, then Galois group of the splitting field of* f *is solvable.*

Remark. The converse of this is also true!

This follows from

Theorem 13.4. *Suppose that* $|\mu_n(k)| = n$*, and* K/k *is a Galois extension such that the Galois group* $\mathrm{Gal}(K/k)$ *is cyclic of order* n*. Then* $K = k(a^{\frac{1}{n}})$ *for some* $a \in k^\times$*. If* $\mathrm{char}(k) = p$*, and* $\mathrm{Gal}(K/k)$ *is cyclic of order* p*, then* K *is the splitting field of* $x^p - x - a$ *for some* $a \in k$*.*

This theorem follows from the following famous result.

Theorem 13.5 (Hilbert's Theorem 90)**.** *Suppose that* K/k *is a Galois extension with cyclic Galois group generated by* σ*. Then*

1. $N_{K/k}(\alpha) = 1$ *iff* $\alpha = \sigma(\beta)/\beta$ *for some* $\beta \in K^\times$*, and*
2. $T_{K/k}(\alpha) = 0$ *iff* $\alpha = \sigma(\beta) - \beta$ *for some* $\beta \in K^\times$*.*

Proof. Recall that

Fact 13.4. *Suppose that* A *is an etale* k*-algebra, and let* k^{sep} *denote the separable closure of* k*. Then*

$$N_{A/k}(\alpha) = \prod_{\sigma \in \mathrm{Hom}(A, k^{sep})} \sigma(\alpha),$$

and

$$T_{A/k}(\alpha) = \sum_{\sigma \in \mathrm{Hom}(A, k^{sep})} \sigma(\alpha).$$

Proving this is quite routine; we just need to show this for the case when A is split etale as $T_{A\otimes k^{\mathrm{sep}}/k^{\mathrm{sep}}}(\alpha\otimes 1) = T_{A/k}(\alpha)$, and in the latter case it is obvious. If we apply it to our case, we see that

$$N_{K/k}(\alpha) = \prod_{\sigma\in \mathrm{Gal}(K/k)} \sigma(\alpha), \quad \text{and} \quad T_{K/k}(\alpha) = \sum_{\sigma\in \mathrm{Gal}(K/k)} \sigma(\alpha)$$

and similarly for trace. This shows one direction.

Now suppose that $T_{K/k}(\alpha) = 0$. By the normal basis theorem, we can choose an element γ such that $\{\sigma^i\gamma\}$ is a basis of K. Write $\alpha = \sum_{i=0}^{n-1} c_i\sigma^i(\gamma)$. Then since trace is linear,

$$T_{K/k}(\alpha) = \sum_{i=0}^{n-1} c_i T_{K/k}(\sigma^i(\gamma)) = (c_0 + \cdots + c_{n-1})T_{K/k}(\gamma).$$

However, the trace form is non-degenerate for separable extensions, so $T_{K/k}(\alpha) = 0$ iff $\sum_{i=0}^{n-1} c_i = 0$. From this, we see that $\alpha = \beta - \sigma(\beta)$, where

$$\beta = c_0\gamma + (c_0 + c_1)\sigma(\gamma) + (c_0 + c_1 + c_2)\sigma^2(\gamma) + \cdots + (c_0 + \cdots + c_{n-1})\sigma^{n-1}(\gamma).$$

The multiplicative case a bit harder to prove. In general, we can show that

Theorem 13.6 (Hilbert's Theorem 90 (Cocycle form))**.** *Let K/k be a Galois extension with Galois group G. Suppose that we have a set $\{a_s\}_{s\in G}$ where $a_s \in K^\times$ such that $a_{st} = a_s\, s(a_t)$. Then there exists $b \in K^\times$ such that $a_s = b^{-1}s(b)$ for all $s \in G$.*

Suppose that $N_{K/k}(\alpha) = 1$. Then since our Galois group is a cyclic group generated by σ, we can define $a_e = 1$ and $a_\sigma = \alpha$, and the rest of the elements must be automatically defined. More explicitly, $a_{\sigma^i} = \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{i-1}(\alpha)$. It is easy to check that this satisfies the condition above by using the fact that the norm is equal to 1. Then the theorem implies that $\alpha = a_\sigma = b^{-1}\sigma(b)$. □

Actually, the cocycle form can be made a little bit simpler if one knows some group cohomology. We start with a definition.

Definition 13.1. Let M be a G-module, i.e., an abelian group equipped with a G-action. We say that a map $\phi : G \to M$ is a *crossed homomorphism* if

$$\phi(gh) = g\phi(h) + \phi(g), \quad \forall g, h \in G.$$

We say that ϕ is a *principal crossed homomorphism* if there exists some $m \in M$ such that $\phi(g) = gm - m$.

It is easy to check that any principal crossed homomorphism is also a crossed homomorphism, but the converse is not true. However, Hilbert's Theorem 90 gives a converse in the case when the G-module is the multiplicative group of a Galois extension.

Theorem 13.7. *Let K/k be a Galois extension with Galois group G. Note that $K^\times$ has a natural G-module structure. Then any crossed homomorphism from G to $K^\times$ is principal.*

We are going to prove the generalized case when K is a Galois G-algebra, and a_s are allowed to be elements of $\mathrm{GL}_n(K)$. In fact, there is yet another form of this theorem.

Definition 13.2. Let M be a K-module. A *descent datum* on M is an action of G on M satisfying $g(\alpha m) = g(\alpha)g(m)$. If M and M' are K-modules with descent datum, then a morphism from $\phi : M \to M'$ is a K-module morphism that is compatible with the group action.

Theorem 13.8 (Hilbert's Theorem 90 (Descent form)). [3] *Let K/k be a Galois G-algebra. Let $\mathcal{C}$ be the category of k-vector spaces and let $\mathcal{D}$ be the category of K-modules with descent datum. Then these two categories are equivalent. The equivalence functor $\mathcal{F}$ from $\mathcal{C}$ to $\mathcal{D}$ is*

$$V \mapsto V \otimes_k K.$$

where the canonical descent datum on the latter is given by

$$g\left(\sum v_i \otimes \alpha_i\right) = \sum v_i \otimes g(\alpha_i).$$

Meanwhile, the functor $\mathcal{G}$ from $\mathcal{D}$ to $\mathcal{C}$ is given by

$$M \mapsto M^G,$$

the submodule of M fixed under G by the action.

[3] This theorem is more well-known as Galois descent. Here are some good notes on this topic.

§ Lecture 14

We will first show that the descent form of Hilbert's Theorem 90 implies the cocycle form.

Proof. Consider K^n, where G acts componentwise. Then define a new action of G on K^n by

$$g * m = a_g g(m).$$

We can do this since $a_g \in M_n(K)$ and $g(m) \in K^n$ so this is just matrix multiplication. We claim that this is a descent datum on K^n. Let's first check that this is an action.

$$s * (t * m) = s * (a_t t(m)) = a_s s(a_t t(m)) = a_s s(a_t) s(t(m)) = a_{st} st(m) = st * m,$$

where we used the fact that $s \in G = \mathrm{Gal}(K/k)$ and hence it preserves field operations. Moreover,

$$s * (am) = a_s s(am) = a_s s(a) s(m) = s(a) a_s s(m) = s(a)(s * m).$$

Note that $s(a) \in K$ so it is a scalar. Therefore, $*$ is indeed a descent datum on K^n.

Now let W be the fixed subspace of K^n, viewed as a k-vector space. Then $W \otimes_k K$ is a K-vector space which, by the descent form, must be isomorphic to K^n as K-vector spaces. Therefore, if we pick a k-basis $\{v_1, \ldots, v_n\}$ of W, it must also be a K-basis of K^n. Now note that for $1 \le i \le m$,

$$v_i = g * v_i = a_g g(v_i),$$

so if we let b' be the matrix with v_i as column vectors, and b be its inverse, then

$$b' = a_g g(b') \implies a_g = b^{-1} g(b), \quad \forall g \in G$$

as desired.[4] □

Finally, here is the proof of the descent form.

Proof of the descent form. We defined the functor $\mathcal{G} : \mathcal{D} \to \mathcal{C}$ by mapping each M to the submodule of M fixed under G-action, say M^G. We first show that $\mathcal{G} \circ \mathcal{F}$ is isomorphic to the identity functor. Note that for any k-vector space V, we have a natural map $V \to (V \otimes_k K)^G$ mapping $v \mapsto v \otimes 1$.

Claim 1. This map is an isomorphism of k-vector spaces.

Proof of Claim 1. Consider a k-basis $\{v_i\}_{i \in I}$ of V. Then $\{v_i \otimes 1\}_{i \in I}$ is a K-basis of $V \otimes_k K$. Now if

$$v = v_1 \otimes k_1 + v_2 \otimes k_2 + \cdots + v_n \otimes k_n,$$

is in $(V \otimes_k K)^G$, then

$$v = gv = v_1 \otimes g(k_1) + v_2 \otimes g(k_2) + \cdots + v_n \otimes g(k_n),$$

which shows that $g(k_i) = k_i$ for all $g \in G$. Since K is a Galois G-algebra, this implies that $k_i \in k$, so $v \in V \otimes_k k$. This gives

$$(V \otimes_k K)^G = V \otimes_k k \cong V.$$ □

For the other direction, note that for any K-module M with descent datum, we have a natural map from $M^G \otimes_k K \to M$ defined by $m \otimes a \mapsto am$ which respects the descent datum.

[4] I finally understood this proof with the help of this comment here.

Claim 2. If K is split, then $M^G \otimes_k K \to M$ is an isomorphism of K-modules.

Proof of Claim 2. Note that any split Galois G-algebra K is of the form k^G, which can be viewed as functions from G to k. If $a \in k^G$ is a function, then the function ga is given by $(ga)(x) = a(g^{-1}x)$. Let M be a K-module. Then if we define $e_x \in K = k^G$ to be $e_x(y) = \delta(xy)$ for all $y \in G$, then

$$M \cong \bigoplus_{x \in G} M_x \coloneqq \bigoplus_{x \in G} e_x M,$$

as K-modules. Now suppose that M has a descent datum. Then $g(e_x m) = g(e_x)g(m) = e_{gx}g(m)$, so the action of g sends M_x to M_{gx}. Hence if we write $N = M_e \subseteq M$, then the above direct sum is the same as

$$M \cong \bigoplus_{x \in G} x(N).$$

Let $m \in M^G$. We can write it uniquely as $m = \sum_{x \in G} x(n_x)$ for $n_x \in N$. Then for all $g \in G$,

$$\sum_{x \in G} x(n_x) = m = g(m) = \sum_{x \in G} gx(n_x) = \sum_{x \in G} x(n_{g^{-1}x}),$$

which implies that n_x is a constant in N independent of x. Hence

$$M^G = \left\{ \sum_{x \in G} xn : n \in N \right\} \cong N.$$

Then the homomorphism maps

$$\sum_{x \in G} xn \otimes e_y \mapsto e_y \cdot \sum_{x \in G} xn = \sum e_y(xn) = yn.$$

So this maps each factor $M_G \otimes e_y K$ of the left direct sum to the factor $y(N)$ of the right one and so it's an isomorphism. □

Claim 3. Let k_1/k be a field extension. Put $K_1 = K \otimes_k k_1$, which is a Galois G-algebra over k_1. Let M be a K-module with descent datum. If we define $M_1 = M \otimes_k k_1 = M \otimes_K K_1$, then the map $\beta : M^G \otimes_k K \to M$ is an isomorphism iff $\beta_1 : M_1^G \otimes_{k_1} K_1 \to M_1$ is an isomorphism.

Proof of Claim 3. We claim that β_1 is just $\beta \otimes \mathrm{id}_{k_1}$. Note that M^G is the kernel of the map $\alpha : M \to \oplus_{x \in G} M$ which maps $m \mapsto (xm - m)_{x \in G}$. Similarly, M_1^G is the kernel of the analogous map α_1. Now M is obtained from M_1 by base change, so it follows that M_1^G is also obtained from M^G via base change, i.e., $M^G \otimes_k k_1$. Therefore,

$$M_1^G \otimes_{k_1} K_1 = M_1^G \otimes_{k_1} k_1 \otimes_k K = M_1^G \otimes_k K = M^G \otimes_k k_1 \otimes_k K = (M_G \otimes_k K) \otimes_k k_1,$$

and under this isomorphism, the map β_1 is just $\beta \otimes \mathrm{id}_{k_1}$. Therefore, β is an isomorphism iff β_1 is an isomorphism. □

Finally, since for any etale algebra we can base change to get a split algebra, we are done. □

§ Lecture 15

We will talk about some applications of the descent theorem described before.

Theorem 15.1. *Let L/k be a finite Galois extension of fields. Let $G = \mathrm{Gal}(K/k)$. Assume that $X \subseteq L^n$ be such that*

(a) X is algebraic; there exist polynomials $f_1, \dots, f_n \in L[x_1, \dots, x_n]$ such that X is the zero locus of this set of polynomials.

(b) Also, $\sigma(X) = X$ for all $\sigma \in G$. Here the action is pointwise.

Then there exist polynomials $g_1, \dots, g_n$ with coefficients in k such that X is the zero locus of these polynomials.

Example 15.0.1. Take $L/k = \mathbb{C}/\mathbb{R}$. Take $X = \{(i, i), (-i, -i)\}$. Then the defining polynomials of X are the four polynomials $(x+i)(y+i)$, $(x+i)(y-i)$, $(x-i)(y+i)$, and $(x-i)(y-i)$. However, we see that this set is also defined by $x - y$ and $x^2 + 1$ which have coefficients in $\mathbb{R}$ instead.

Proof. Let I be the ideal of $L[x_1, \dots, x_n]$ consisting of all the polynomials that vanish on X. We can define the G-action on $L[x_1, \dots, x_n]$ by applying $\sigma \in G$ to the coefficients. This maps I to itself since if a polynomial f vanishes on the set X, then $\sigma(f)$ vanishes on $\sigma(X) = X$.

Note that $L[x_1, \dots, x_n] = k[x_1, \dots, x_n] \otimes_k L$, and this has canonical descent datum given as above. Moreover, we can restrict this to get a descent datum on the ideal I, as $\sigma(I) = I$ for all $\sigma \in G$. Then by the descent theorem, $I = I_0 \otimes_k L$, where I_0 is an ideal of $k[x_1, \dots, x_n]$. This ring is Notherian, so the ideal I_0 has finitely many generators. These generators are precisely the polynomials $g_1, \dots, g_n$ that we want. □

Theorem 15.2 (Skolem-Noether)**.** *Let L/k be a finite Galois extension. Let A be a finite dimensional k-algebra such that $A \otimes_k L \cong M_n(L)$. Then every k-algebra automorphism of A is inner; i.e., there exists $g \in A^\times$ such that $\alpha(a) = gag^{-1}$.*

Proof. Suppose that we have proven the case when $A = M_n(k)$ is a matrix algebra. Let α be an automorphism of A. Then $\alpha \otimes \mathrm{id} \coloneqq \alpha_L$ is an automorphism of the L-algebra $A \otimes_k L \cong M_n(L)$. Therefore, there exists an invertible element $g \in (A \otimes_k L)^\times \coloneqq A_L^\times$ such that $\alpha_L(a) = gag^{-1}$. Note that $\sigma(\alpha_L) = \alpha_L$ for all $\sigma \in G = \mathrm{Gal}(L/k)$ (here σ is acting on A_L as $\mathrm{id} \otimes \sigma$.) Therefore, for all elements $a \in A_L$,

$$\sigma(\alpha_L)(a) = \sigma(\alpha_L(\sigma^{-1}(a))) = \sigma(g\sigma^{-1}(a)g^{-1}) = \sigma(g)a\sigma(g)^{-1} = gag^{-1}.$$

Therefore, $g^{-1}\sigma(g)$ lies in the center of A_L. However, $Z(A_L) = L^\times$, so $g^{-1}\sigma(g) = c_\sigma$ for some $c_\sigma \in L^\times$. Now note that $(c_\sigma)_{\sigma \in G}$ is a cocycle, since

$$c_\sigma \sigma(c_\tau) = g^{-1}\sigma(g)\sigma(g^{-1}\tau(g)) = g^{-1}\sigma\tau(g) = c_{\sigma\tau}.$$

Therefore, by Hilbert's Theorem 90, there exists $b \in L^\times$ such that $c_\sigma = b^{-1}\sigma(b)$. However, by definition, $c_\sigma = g^{-1}\sigma(g)$, so $gb^{-1} = \sigma(gb^{-1})$. Therefore, $gb^{-1} \in (A \otimes_k L)^{\times G} = A^\times$. Hence,

$$\sigma(a) = gag^{-1} = gb^{-1}abg^{-1} = g_1 a g_1^{-1},$$

where $g_1 \in A^\times$ as desired.

It remains to prove this for the case when A is a matrix algebra itself. We will continue this after proving some necessary tools. □

Theorem 15.3 (Morita equivalence). *Let R be a ring. There is an equivalence between the category of left R-modules and the category of left $M_n(R)$-modules. The functors are given by $V \mapsto V^n$, and $M \mapsto e_{11}M$.*

Proof. Note that $e_{11}V^n = V \oplus 0 \oplus \cdots \oplus 0$, and this is naturally isomorphic to V. Now let M be a $M_n(R)$-module. Note that if M is an $M_n(R)$-module, then $M = \bigoplus_{i=1}^n e_{ii}M$. However, $e_{ii}(M) \cong e_{jj}(M)$ simply by multiplication with e_{ji}, so this gives me a natural R-module isomorphism $f_M : \bigoplus_{i=1}^n e_{11}M \to \bigoplus_{i=1}^n e_{ii}M$. It can be checked that this is in fact an isomorphism of $M_n(R)$-modules. This completes the proof. □

Remark. Here is a more symmetric description of the two equivalence functors. Let $C_n = R^n$ as column vectors. This is both a left $M_n(R)$-module and an right R-module. If we instead consider $R_n = R^n$ as row vectors, then this is a $(R, M_n(R))$-bimodule instead. If V is a left R-module, then we can form the tensor product $C_n \otimes_R V$ which is a left $M_n(R)$-module. Now if M is a left $M_n(R)$-module, then we can form the tensor product $R_n \otimes_{M_n(R)} M$, which is a left R-module. It turns out that these are precisely the two equivalence functors that appeared above. The Morita equivalence is just the fact that

$$R_n \otimes_{M_n(R)} C_n \cong R$$

as (R, R)-bimodules, and

$$C_n \otimes_R R_n \cong M_n(R)$$

as $(M_n(R), M_n(R))$-bimodules.

Fact 15.1. *Let k be a field. Then any k-linear equivalence (this means that the equivalence produces linear maps between hom-sets) from the category of k-modules to itself is naturally isomorphic to the identity functor.*

Once we know this, we can finish the proof of Skolem-Noether theorem.

Proof of Skolem-Noether continued. Let α be an automorphism of $M_n(k)$. For any $M_n(k)$-module M, let $\alpha^*(M)$ be the $M_n(k)$-module such that the underlying k-module is M and the new scalar multiplication is defined by $a \cdot m = \alpha(a)m$. Then the functor α^* is a k-linear self-equivalence of category of $M_n(k)$-modules. By the Morita equivalence and the fact above, it follows that α^* must be naturally isomorphic to the identity functor of the category of $M_n(k)$-modules; let this natural isomorphism be ϕ. Note that this ϕ can be regarded as an automorphism of the forgetful functor from the category of $M_n(k)$-modules to the category of k-modules since both M and α^*M have the same k-module structure (the 'twisting' effect of α only occurs for elements outside of k.) However, this automorphism group is the same as $M_n(k)^\times$. Therefore, there exists $b \in M_n(k)^\times$ such that $\phi_M(m) = bm$ for all m and all M. Now note that

$$bam = \phi_M(a \cdot m) = a \cdot \phi(m) = \alpha(a)bm$$

for all a and for all m. Therefore, this implies that $\alpha(a) = bab^{-1}$ as desired. □

§ Lecture 16

From now on, we will focus on central simple algebras.

Definition 16.1. Let k be a field. A k-algebra A is called *central* if $Z(A) = k$.

Remark. Note that these two conditions are stable under base change. i.e., Given a field extension k'/k, A is central iff $A \otimes_k k'$ is central and similarly for finiteness.

Theorem 16.1. *Let A be a finite dimensional central k-algebra. Then TFAE:*

(1) The only two-sided ideals of A are $\{0\}$ and A.

(2) $A \otimes_k A^{op} \cong M_n(k)$ where $n = \dim_k A$.

(3) $A \cong M_n(D)$ where D is a central division k-algebra.

(4) The category of A-modules is semisimple[5] with only one isomorphism class of simple modules.

(5) There exists a field extension k'/k such that $A \otimes_k k' \cong M_n(k')$.

(6) There exists a finite separable extension k'/k such that $A \otimes_k k' \cong M_n(k')$.

If A satisfies any of the above properties, then we say that A is a central simple k-algebra. If $A \cong M_n(k)$, then we say that A is split.

Corollary 16.1.1. *If A and A' are central simple algebras, then $A \otimes_k A'$ is also a central simple algebra.*

We will prove this theorem later; we will state other interesting theorems about CSAs first.

Theorem 16.2. *Let A and A' be CSAs over k. Then TFAE:*

(1) $A \otimes (A')^{op}$ is split.

(2) There exists a CDA D such that $A \cong M_n(D)$ and $A' \cong M_{n'}(D)$.

(3) There exists $m, m' > 0$ such that $M_{m'}(A) \cong M_m(A')$.

(4) A-Mod is equivalent to A'-Mod as k-linear categories.

Write $A \sim A'$ if these are satisfied. Then $\sim$ is an equivalence relation on the category of k-CSAs up to isomorphism.

Theorem 16.3. *Let A and A' be defined as follows. Then the equivalence class of $A \otimes_k A'$ depends only on the equivalence classes of A and A'.*

This means that we can define a binary operation on the set of equivalence classes of central simple algebras.

Definition 16.2. This set along with the binary operation forms a commutative group! This group is called the *Brauer group* of field k, denoted by $\mathrm{Br}(k)$.

We will discuss about simple and semisimple modules before we prove all of these.

[5] This means that every A-module is semisimple.

Definition 16.3. Let R be any ring. A R-module S is called *simple* if the only R-submodules of S are $\{0\}$ and S, and S is not the zero module.

Lemma 16.4. *Every such S is isomorphic to R/M where M is a maximal left ideal of R.*

Proof. Let x be a non-zero element of S. Then the R-submodule generated by x must be the whole of S. Therefore, if we define the map $\phi : R \to S$ defined by $a \mapsto ax$, then ϕ is surjective, and so $S \cong R/\ker(\phi)$, and it must be maximal since any ideal that lies between R and $\ker(\phi)$ corresponds to a R-submodule of S. □

Lemma 16.5 (Schur). *Let S and S' be simple R-modules, and suppose that $f : S \to S'$ is an R-module homomorphism. Then either f is the zero map or it is an isomorphism.*

Proof. This is actually trivial. □

As a corollary, we get

Corollary 16.5.1. *If S is a simple R-module, then $\mathrm{End}_R(S)$ is a division ring.*

Remark. Let R be a k-algebra where k is an algebraically closed field, and let S be a simple module whose dimension over k is finite. Then $\mathrm{End}_R(S) = k$. To see this note that for each $a \in k$ we can define $s \mapsto as$ which is an element of $\mathrm{End}_R(S)$, so $k \subset \mathrm{End}_R(S)$. Conversely, let $f \in \mathrm{End}_R(S)$. Then we can find an eigenvalue λ of f as a k-linear map. Then $f - \lambda\,\mathrm{id}$ is an element of the endomorphism ring $\mathrm{End}_R(S)$, but this is not invertible as a k-linear map so certainly not as a ring map, so by Schur's lemma it must be the zero map, i.e., $f = \lambda\,\mathrm{id}$ for some $\lambda \in k$.

Theorem 16.6. *Let R be a ring and M be an R-module. Then TFAE:*

(1) M is a sum of simple submodules.

(2) M is a direct sum of simple submodules.

(3) Every submodule of M is a direct summand of M.

Definition 16.4. We say that M is *semisimple* if the conditions above are satisfied.

Proof. It is obvious that (2) ⇒ (1). We now show that (1) ⇒ (3), so suppose that $M = \sum_{i\in I} S_i$ where each S_i is simple. Let M' be a submodule of M, our goal is to find a submodule M'' such that $M = M' \oplus M''$. Consider $C = \{J \subset I : \sum_{j\in J} S_j \text{ is direct and } \sum_{j\in J} S_j + M' \text{ is direct}\}$. The condition that $\sum_{j\in J} S_j$ is direct just means that the map $\bigoplus_{j\in J} S_j \to M$ defined by summation is injective. Then C is a poset satisfying the conditions of Zorn's lemma, and so there exists a maximal element $J_0 \subset I$.
Claim 1. Let $M'' = \bigoplus_{j\in J_0} S_j$. Then $M'' \oplus M' = M$.

Proof. Assume that there exists some $i_0 \in I$ such that S_{i_0} is not contained in LHS. Clearly $i_0 \notin J$. Then the intersection of LHS and S_{i_0} must be the zero module, so $M'' + S_{i_0} = M'' \oplus S_{i_0}$. Therefore, $J_0 \cup \{i_0\}$ is strictly bigger than J which is a contradiction. Therefore, each S_i is contained in the LHS, which means that M must also be contained in it. This finishes the proof. □

We now prove that (3) ⇒ (1). Suppose that every submodule of M is a direct summand of M. Then every submodule of M have the same property too. To see this let M' be a submodule of M and M'' be a submodule of M'. Then there exists a submodule P of M such that $M = M'' \oplus P$.

We now claim that $M' = M'' \oplus (M' \cap P)$. This is actually quite obvious: for $m' \in M'$, we can write it uniquely as $m' = m'' + p$, and this implies that $p \in M' \cap P$ since $m'' \in M'$.

Now we construct a sum of simple submodules which is equal to M. Let $M_0 = \sum_{S \subset M} S$, where S is a simple submodule of M. If M_0 is not the whole M, then $M = M_0 \oplus L$ for some non-zero submodule L. Then take some non-zero $x \in L$. Then Rx is isomorphic to R/I for some ideal I and so it follows that Rx has a simple quotient. Then the above observation implies that Rx has a simple R-submodule (more specifically, the kernel of the quotient map is a direct summand of Rx, we can just take the other summand of this direct sum) and which is a contradiction.

Now we just need to prove (1) $\Rightarrow$ (2). But we can just take the zero submodule at the start in the proof of (1) $\Rightarrow$ (3) and this would imply that M'', which is a direct sum of simple modules, is equal to M itself. □

We can now prove the characterization theorem for central simple algebras. We first verify it for some special cases.

Lemma 16.7. *Property (4) is satisfied if $A = M_n(D)$ where D is a division algebra.*

Proof. This follows from the Morita equivalence. Note that this property remains unchanged under an equivalence of categories, and so we just need to show it for the category of D-modules. But in this case we can employ the theory of vector spaces over division rings. □

Lemma 16.8 (Rieffel)**.** *Let R be a ring that has only $\{0\}$ and R as two-sided ideals. Let L be a non-zero left ideal. We can view L as a left $\mathrm{End}_R(L)$-module, and there is a natural map $\lambda : R \to \mathrm{End}_{\mathrm{End}_R(L)}(L)$ given by left multiplication with elements of R. This map is an isomorphism.*

Proof. λ is certainly injective since $\ker \lambda$ is a two-sided ideal, and it is not equal to R since $1 \mapsto \mathrm{id}$, so the kernel must be trivial. Therefore, we just need to show that λ is surjective. Note that for any left-ideal L, LR is a two-sided ideal of R, and it is non-zero so it must be the whole ring. Therefore, we can write $1 = \sum_{i=1}^n x_i y_i$ where $x_i \in L$ and $y_i \in R$. Applying λ to both sides gives

$$\mathrm{id} = \sum_{i=1}^n \lambda(x_i)\lambda(y_i),$$

so it follows that $\mathrm{id} \in \mathrm{Im}(LR)$.

We now claim that $\mathrm{Im}(L)$ is a left ideal of $\mathrm{End}_{\mathrm{End}_R(L)}(L)$. Let $f \in \mathrm{End}_{\mathrm{End}_R(L)}(L)$, and consider $f \circ \lambda(x)$ where $x \in L$. Then since multiplication by y on the right is an endomorphism in $\mathrm{End}_R(L)$, we see that

$$(f \circ \lambda(x))(y) = f(xy) = f(x)y = \lambda(f(x))(y),$$

so $f \circ \lambda(x) \in \lambda(L)$.

Therefore, $\mathrm{Im}(LR)$ is also a left-ideal, and since it contains id, it must be the whole ring. Therefore, λ is surjective, and this completes the proof. □

§ Lecture 17

We are going to apply Rieffel's lemma in the case when $A = M_n(D)$ for some central division ring D. By Morita Equivalence, any A-module M is of the form S^m, where S is the unique simple A-module which we can take to be the space of column vectors D^n. Then $\mathrm{End}_A(M) = M_m(D^{\mathrm{op}})$.

We now start proving Theorem 16.1.

Proof. Let's show that (1) $\Rightarrow$ (3). Let L be a minimal non-zero left ideal of A. Then L is a simple A-module, and so by Schur's lemma, $\mathrm{End}_A(L)$ is a division ring. Therefore, applying Rieffel's lemma shows that

$$A \cong \mathrm{End}_{\mathrm{End}_A(L)}(L) = \mathrm{End}_D(L),$$

Then $L = D^n$ for some integer n since it is a D-vector space, so $\mathrm{End}_D(L) \cong M_n(D^{\mathrm{op}})$.

To see (3) $\Rightarrow$ (1), we apply the Morita equivalence. Let $A = M_n(D)$ for some central division algebra D. Then a left ideal of A is of the form $\mathrm{Hom}_D(D^n, W)$ where W is a D-submodule of D^n. Now note that such a left-ideal is a two-sided ideal only when W is zero or the whole ring. This shows that A is simple. Moreover, the center of $M_n(D)$ is the same as the center of D, which is just k.

(3) $\Rightarrow$ (4) was proven in a remark above.

Now we show that (3) $\Rightarrow$ (5). Let A be a k-CSA, and let k' be an algebraic closure of k. Then by the lemma below, $A' = A \otimes_k k'$ is a central simple k'-algebra, so it must be of the form $M_n(D)$, where D is a central division k'-algebra. Schur's lemma then tells us that $D = k'$, so $A \otimes_k k' = M_n(k')$ (see the remark after Corollary 16.5.1.)

Also, (5) $\Rightarrow$ (3) follows readily from Lemma 17.1 since $M_n(k')$ is a central simple k'-algebra for any field extension k' of k.

(1) $\Rightarrow$ (2) is proved more specifically as Fact 17.1 below.

Let's now prove (2) $\Rightarrow$ (1). If A is not simple, then there is a non-zero proper two-sided ideal I of A. If A and B are k-algebras and I and J are two-sided ideals of A and B respectively, then $I \otimes_k J$ is also a two-sided ideal of $A \otimes_k B$. In our case when $B = A^{\mathrm{op}}$, $I \otimes_k A^{\mathrm{op}}$ is a non-zero proper two-sided ideal of $A \otimes_k A^{\mathrm{op}}$, which is a contradiction as the latter ring is simple.

To prove (4) $\Rightarrow$ (3), recall that for any ring A, $\mathrm{End}_A(A) = A^{\mathrm{op}}$ if we view A as a left A-module. Let S be an object from the unique isomorphism class of simple A-modules. Then A as a left A-module is isomorphic to S^n for some n. Since $\mathrm{End}_A(S^n) = M_n(\mathrm{End}_A(S))$ and $\mathrm{End}_A(S)$ is a division ring by Schur's lemma, it follows that A^{op} is a matrix ring over a division ring. Therefore, A itself must also be a matrix ring over a division ring.

Finally, (5) $\Rightarrow$ (6) is proved below as a separate theorem. □

Lemma 17.1. *Let A be a finite-dimensional k-algebra, and let k'/k be a field extension. Then A is a k-CSA iff $A \otimes_k k'$ is a k'-CSA. In other words, the property of being a CSA is stable under base change.*

Proof. Note that A is a central k-algebra iff $A \otimes_k k'$ is a central k'-algebra, so we just need to check that base change preserves simplicity.

First, assume that $A \otimes_k k'$ is a k'-CSA. Let I be a non-zero ideal of A. Then $I \otimes_k k'$ is contained in $A \otimes_k k'$ and it is also a non-zero ideal of $A \otimes_k k'$, so it must be the whole ring. This implies that $I = A$ since $\dim_k I = \dim_k A$.

Now suppose that A is a k-CSA, and let I be a non-zero ideal of $A \otimes_k k'$. Let m be the smallest possible integer such that there exists some non-zero $\alpha \in I$ such that $\alpha = \sum_{i=1}^n a_i \otimes b_i$, for some

$a_i \in A$ and $b_i \in k'$. Then by the minimality of n, $a_1, \ldots, a_n$ are linearly independent in A over k and $b_1, \ldots, b_n$ are linearly independent in k' over k.

Now consider the set Aa_1A, which is a two-sided non-zero ideal of A. Then as A is simple, this ideal must be the whole ring, so there exist $x_i, y_i \in A$ such that

$$\sum_{j=1}^{m} x_j a_1 y_j = 1.$$

Now consider

$$\sum_{j=1}^{m} (x_j \otimes 1)\alpha(y_j \otimes 1) = \sum_{i=1}^{n}\sum_{j=1}^{m} x_j a_i y_j \otimes b_i = \sum_{i=1}^{n} a_i' \otimes b_i = \alpha'.$$

which is still an element of I with minimal length, but now $a_1 = 1$. Therefore, we can just assume from the start that $a_1 = 1$. Now suppose that $n > 1$. Then a_2 and a_1 are linearly independent over k, so it follows that $a_2 \notin k = Z(A)$. This means that there exists some $b \in A$ such that $a_2 d \neq d a_2$. However, if we consider the element $(d \otimes 1)\alpha - \alpha(d \otimes 1)$, then this can be written as

$$\sum_{i=1}^{n} (da_i - a_i d) \otimes b_i.$$

From this, it is clear that this element has length smaller than n and is non-zero since the coordinate of b_1 is zero but the coordinate of b_2 is non-zero. This contradicts the minimality of n, so it follows that $n = 1$. Therefore, I contains an element of the form $1 \otimes b_1$ where $b_1 \neq 0$. It is evident that any two-sided ideal containing such an element must be the whole ring. □

Fact 17.1. *Let A be a finite dimensional k-algebra. Let $A_\circ$ be the underlying k-vector space of A. Let ϕ be the map defined by*

$$\begin{aligned} \phi : A \times A^{op} &\to \mathrm{End}_k(A_\circ) \\ (\alpha, \beta) &\mapsto (x \mapsto \alpha x \beta) \end{aligned}$$

This map is k-bilinear, so this gives a k-linear map Φ from $A \otimes_k A^{op} \to \mathrm{End}_k(A_\circ)$ which is a k-algebra homomorphism. If A is a k-CSA, then Φ is an isomorphism.

Proof. Let A be a k-CSA, and let k' be such that $A' = A \otimes_k k' = M_n(k')$. Then to show that Φ_A is an isomorphism is the same as showing that $\Phi_A \otimes \mathrm{id} : (A \otimes_k A^{\mathrm{op}}) \otimes_k k' \to \mathrm{End}_k(A_\circ) \otimes_k k'$ is an isomorphism. But this map is the same as $\Phi_{A'}$. Therefore, we just need to prove this fact in the case when A is a matrix algebra.

So, suppose that $A = M_n(k)$. Then $A^{\mathrm{op}} \cong M_n(k)$ by tranposing, so it follows that $A \otimes_k A^{\mathrm{op}} = M_n(k) \otimes_k M_n(k) \cong M_{n^2}(k)$. Meanwhile, $\mathrm{End}_k(A_\circ) = M_{n^2}(k)$. The map Φ is a k-algebra map whose kernel is non-zero, and since $M_{n^2}(k)$ is simple, it follows that Φ is one-to-one. Since the domain and codomain have the same dimension as k-vector spaces, it then follows that Φ is indeed an isomorphism. □

Before we prove the final part, we need the following lemma.

Lemma 17.2. *Let A be a k-CSA with dimension n^2. Assume $k' \subset A$ is a k-subalgebra such that k'/k is a field extension of degree n. Then $A \otimes_k k' \cong M_n(k')$.*

Proof. Note that k' is also a k-subalgebra of A^{op}. Therefore, $A \otimes_k k'$ is a k-subalgebra of $A \otimes_k A^{\mathrm{op}} \cong \mathrm{End}_k(A_\circ)$. By right multiplication by elements of k', we can view A as a k'-vector space, say A', and it is immediate that $\mathrm{End}_{k'}(A') \subset \mathrm{End}_k(A_\circ)$, and $A \otimes_k k' \subset \mathrm{End}_{k'}(A')$. In fact this latter inclusion is an equality for dimension reasons (both have dimension n^2 over k'). The latter is obviously a matrix algebra over k', and $\dim_{k'} A = n$, so this is just $M_n(k')$. $\square$

§ Lecture 18

Here is a brief review about discriminants. Recall that the *discriminant* is a unique polynomial in n variables with integer coefficients, such that for any degree n polynomial $f = x^n - c_1 x^{n-1} + c_2 x^{n-2} + \cdots \pm c_n$ whose roots are α_i, then

$$\mathrm{Disc}(c_1, \ldots, c_n) = \prod_{i>j} (\alpha_i - \alpha_j)^2.$$

Theorem 18.1 (Noether, Koethe). *Let A be a k-CSA of dimension n^2. Then there exists a finite separable extension k'/k such that $A \otimes_k k' \cong M_n(k')$.*

Proof. It is enough to handle the case when A is a division algebra. Also we can assume that k is infinite since the theorem is obvious for finite fields which are perfect. By the lemma above, it suffices to find a separable extension of degree n contained inside D. Choose K/k such that $A \otimes_k K \cong M_n(K)$ and denote the isomorphism by ϕ. For $\alpha \in A$, we want to look at the discriminant of the charactersitic polynomial of $\phi(\alpha \otimes 1)$. If we fix a basis $v_1, \ldots, v_N$ of A over k, then we can write $x = \sum_{i=1}^N a_i (v_i \otimes 1)$ for all $x \in A \otimes_k K$ with coefficients in K. Then the discriminant is a polynomial of these coefficients, say $f(a_1, \ldots, a_n)$ in $K[x_1, \ldots, x_n]$. If this polynomial is the zero polynomial, then $\phi(x)$ has discriminant 0 for all $x \in A \otimes_k K$. But $\phi(A \otimes_k K) = M_n(K)$ and there are certainly matrices with separable characteristic polynomial. Therefore, f is not the zero polynomial, and since the field k is infinite, it follows that f does not vanish on k^n, and therefore, there exists $\alpha \in A$ such that $\phi(\alpha \otimes 1)$ has a separable characteristic polynomial.

Now fix such an $\alpha \in A$. We claim that the subring of A generated by α over k is a separable field extension of k of degree n. This ring is automatically a field because it is a commutative integral domain which is finite-dimensional over k, and so it is isomorphic to $k[x]/(f)$ where f is the irreducible polynomial of α over k. Denote this field by F.

Note that A can be regarded as an F-vector space. If we consider the k-linear transformation $\rho_\ell(\alpha) : A \to A$ by left multiplication with α, then we see that the minimal polynomial of this transformation is the same as f. However, we can find this minimal polynomial in another way; since ϕ is an isomorphism, this is the same as the minimal polynomial of $\rho_\ell(\phi(\alpha \otimes 1))$ in $M_n(K)$, which is just the minimal polynomial of the matrix $\phi(\alpha \otimes 1)$ (this is not completely trivial!) However, by our assumption, the latter is a separable monic polynomial of degree n, so we're done. □

Definition 18.1. Let X, X' be certain 'structures' defined over a field k. We say that X, X' are twists of each other if there exists a field extension such that $X \otimes_k k' \cong X' \otimes_k k$.

Example 18.1.1. Etale algebras are twists of split etale algebras. Any non-degenerate quadratic form over $\mathbb{R}$ is a twist of $x_1^2 + \cdots + x_n^2$. $U(n)$ is a twist of $\mathrm{GL}(n, \mathbb{R})$. Every CSA over k is a twist of $M_n(k)$.

Remark. If we know that the twisting can be achieved using k' separable/Galois over k, we can study them using Galois theory.

Since we have some time left, Professor Yu decided to prove this classic theorem for entertainment purposes.

Theorem 18.2. *Let k be a field, and let $e_1, \ldots, e_n$ be elementary symmetric polynomials. Then any symmetric polynomial can be written as a polynomial of elementary symmetric polynomials.*

Proof. The fact that the right side is included in the left side is obvious. Now if we consider the extension $k(x_1, \ldots, x_n)/k(e_1, \ldots, e_n)$, this is a separable extension of degree at most $n!$, since it is the splitting field of $\prod_{i=1}^{n}(X - x_i)$. However, there are at least $n!$ automorphisms fixing k, so it follows that this is a Galois extension, and that the fixed field is exactly the base field. In other words, any rational symmetric function is a rational polynomial of elementary symmetric polynomials.

In order to show our conclusion, we just need to show that $k[x_1, \ldots, x_n] \cap k(e_1, \ldots, e_n) = k[e_1, \ldots, e_n]$. I cannot quite recall how Professor Yu did it, but here is a proof that uses integral extensions. Note that the ring extension $k[e_1, \ldots, e_n] \subset k[x_1, \ldots, x_n]$ is an integral extension, since each x_i is a root of the monic polynomial $\prod_{i=1}^{n}(X - x_i) \in k[e_1, \ldots, e_n][X]$. If f belongs to the left hand side, then f is integral over $k[e_1, \ldots, e_n]$ and $f \in k(e_1, \ldots, e_n)$. However, $k[e_1, \ldots, e_n]$ is integrally closed (since $e_1, \ldots, e_n$ are algebraically independent and so it is isomorphic to $k[x_1, \ldots, x_n]$ which is a UFD), and so it follows that $f \in k[e_1, \ldots, e_n]$. $\square$

§ Lecture 19

Recall the following theorem that we stated during a previous lecture.

Theorem 19.1. *Let A, A' be k-CSAs. Then TFAE:*

(1) $A \cong M_n(D)$ and $A' \cong M_{n'}(D)$.

(2) There exist n, n' such that $M_n(A) \cong M_{n'}(A')$.

(3) $A \otimes (A')^{op}$ is a matrix algebra.

(4) The categories ${}_A\mathsf{Mod}$ and ${}_{A'}\mathsf{Mod}$ are equivalent as k-linear categories.

We say that A and A' are *Brauer-equivalent* if these conditions are satisfied.

Proof. Let's show that (1) $\Rightarrow$ (3). Suppose $A = M_n(D)$ and $A' = M_{n'}(D)$ for some integers n and n'. Then

$$A \otimes_k (A')^{\mathrm{op}} = M_n(D) \otimes M_{n'}(D)^{\mathrm{op}} = M_n(k) \otimes D \otimes M_n(k) \otimes D^{\mathrm{op}} = M_{nn'}(k) \otimes M_{d^2}(k) = M_{d^2nn'}(k)$$

where we used the fact that $D \otimes D^{\mathrm{op}} = M_{d^2}(k)$ where d is the dimension of D over k.

To show (3) $\Rightarrow$ (1), we note that

$$M_{N'}(D^{\mathrm{op}}) = D^{\mathrm{op}}A \otimes A \otimes A'^{\mathrm{op}} = M_n(k) \otimes A\text{"op} = M_{Nn'}(D'^{\mathrm{op}})$$

so by the lemma below we see that $D \cong D'$.

(1) $\Rightarrow$ (2) is trivial, and (4) $\Rightarrow$ (1) and (2) $\Rightarrow$ (4) follow from the Morita equivalence. □

Lemma 19.2. *Let A be a CSA over k. Suppose $A \cong M_n(D)$ and $A \cong M_{n'}(D')$. Then $n = n'$ and $D \cong D'$ as k-algebras.*

Therefore, there is a bijection between the k-CSAs up to Brauer equivalence and k-CDAs up to isomorphism. This will allow us to define a group structure on the latter set, which is not closed under tensor product.

Theorem 19.3. *The set of k-CSAs up to Brauer equivalence has an abelian group structure given by $[A] \cdot [A'] = [A \otimes_k A']$.*

Proof. First, let's show that this is well-defined. Suppose that $A \sim A'$ and $B \sim B'$. To see if $A \otimes_k B \sim A' \otimes_k B'$, we just compute the tensor product

$$\begin{aligned}(A \otimes_k B) \otimes_k (A' \otimes_k B')^{\mathrm{op}} &= (A \otimes_k B) \otimes_k (A'^{\mathrm{op}} \otimes_k B'^{\mathrm{op}}) \\ &= (A \otimes_k A'^{\mathrm{op}}) \otimes_k (B \otimes_k B'^{\mathrm{op}}) = M_n(k) \otimes M_{n'}(k) = M_{nn'}(k),\end{aligned}$$

and since this is a matrix algebra, they are indeed Brauer equivalent.

The binary operation defined is both commutative and associative since the tensor product satisfies these properties. The identity element is just the class of $[k]$, since $A \otimes_k k = A$ for all k-algebras A. The inverse is given by A^{op} since

$$[A] \cdot [A^{\mathrm{op}}] = [A \otimes_k A^{\mathrm{op}}] = [M_n(k)] = [k].$$ □

Definition 19.1. This group is called the *Brauer group* of the field k, denoted by $\mathrm{Br}(k)$.

Now let K/k be a field extension. As noted before, any central simple k-algebra A remains a CSA after base change to K. After some checking we can see that the map $[A] \in \mathrm{Br}(k) \mapsto [A \otimes_k K] \in \mathrm{Br}(K)$ is well-defined and is a group homomorphism.

Definition 19.2. The kernel of this map is called the *relative Brauer group* of the field extension K/k.

In other words, the relative Brauer group consists of the equivalence classes of k-CSAs that become a matrix algebra over K after base change.

Remark. k-CSAs are just k-algebras which are "locally (in the etale topology) is a matrix algebra".

To proceed further, we introduce some terminology from group cohomology.

Definition 19.3. A *G-module* is an abelian group A equipped with an action of G. In other words, it is just the data of a group homomorphism from G to $\mathrm{Aut}(A)$.

Given a G-module A, we can consider the following chain complex, whose i-th element is $C^i(G, A)$ consisting of all functions from G^i to A. We call the elements of $C^i(G, A)$ to be *i-cochains*. Then there are *coboundary maps* $\delta^n : C^n(G, A) \to C^{n+1}(G, A)$ between the objects defined by

$$\delta^n(f)(g_0, \ldots, g_n) \coloneqq g_0 f(g_1, \ldots, g_n) - f(g_0 g_1, g_2, \ldots, g_n) + f(g_0, g_1 g_2, \ldots, g_n) + \\ \cdots + (-1)^n f(g_0, \ldots, g_{n-2}, g_{n-1} g_n) + (-1)^{n+1} f(g_0, \ldots, g_{n-1}).$$

and we attach the map $0 \to C^0(G, A)$ to the chain complex. The key thing is that $\delta^i \circ \delta^{i-1} = 0$, so $\operatorname{im} \delta^{i-1} \subset \ker \delta^i$ for all $i \geq 0$.

Definition 19.4. The i-th cohomology group is defined to be $\ker \delta^i / \operatorname{im} \delta^{i-1}$, and is denoted by $H^i(G, A)$.

Remark. The 0-th cohomology group is just A^G, the set of elements of A fixed by G. This is not a coincidence! The morally correct definition of cohomology groups is to define them as the right derived functors of the left exact functor $A \mapsto A^G$ from G-Mod to Ab. In particular, there is a long exact sequence connecting all the cohomology groups.

Remark. If A is not abelian, we can still define the first cohomology group $H^1(G, A)$. We just define it to be the kernel of δ^1 modulo the relation that $f \sim g$ iff there exists an element $\alpha \in A$ such that $\alpha f(s) s(\alpha)^{-1} = g(s)$ for all $s \in G$. However, we only define up to the first cohomology group for nonabelian G-modules (which we will call G-groups instead.)

Here is the reason why we introduced these cohomology groups.

Theorem 19.4. *Let K/k be a finite Galois extension, and let $G = \mathrm{Gal}(K/k)$. Then there is a natural isomorphism between*

$$\mathrm{Br}(K/k) \cong H^2(G, K^\times).$$

Proof. Let's first construct the map from $\mathrm{Br}(K/k) \to H^2(G, K^\times)$. Let A be a k-CSA such that $M_n(K) \cong A \otimes_k K$. Let this isomorphism be ϕ. For an element $s \in G$, define $a_s = \phi^{-1} s(\phi) : M_n(K) \to M_n(K)$[6]. This is a k-algebra automorphism of $M_n(K)$, and by Noether-Skolem theorem, we can identity the group $\mathrm{Aut}_K(M_n(K))$ with the group $\mathrm{GL}_n(K)/K^\times$.

[6] We have a natural map from G to $\mathrm{Aut}(A \otimes_k K)$ defined by $s \mapsto \mathrm{id} \otimes s$ for all $s \in G$. We then have an action of s on $\mathrm{Hom}_k(M_n(K), A \otimes_k K)$ defined by $(s\phi)(x) = s(\phi(s^{-1}(x)))$.

We can check that a_s is a cocycle in $C^1(G, \mathrm{GL}_n(K)/K^\times)$. Now using the exact sequence $0 \to K^\times \to \mathrm{GL}_n(K) \to \mathrm{GL}_n(K)/K^\times \to 0$, we can lift the 1-cocycle to a 2-cocycle in $C^2(G, K^\times)$ by using the snake lemma. Explicity, this is given by

$$c_{s,t} = s(\tilde{a}_t)(\tilde{a}_{st})^{-1}(\tilde{a}_s)$$

where $\tilde{a}_s$ denotes the lift of a_s in $\mathrm{GL}_n(K)$. We then define the map $\beta : \mathrm{Br}(K/k) \to H^2(G/K^\times)$ as

$$\beta([A]) = (c_{s,t}) \mod B^2,$$

where $B^2 = \operatorname{im} \delta^1$.

The fact that this map is well-defined is shown in two steps in the lemma below. Unfortunately, we do not have time to check that this is a group isomorphism. Basically, the injectivity is by Hilbert's Theorem 90, and the surjectivity is by constructing the crossed product algebra. □

Lemma 19.5 (First stage). *Let X be an object over k. Then consider the set of K/k-twists of X up to k-isomorphism. There is a natural map from this set to $H^1(G, \mathrm{Aut}_K(X \otimes_k K)$.*

Proof. Given X'/k, there is an isomorphism $\phi : X \otimes_k K \to X' \otimes_k K$. Then for any $s \in G$, we can define $a_s = \phi^{-1} s(\phi) \in \mathrm{Aut}_k(X \otimes_k K)$. We claim that this is a 1-cocycle from G to $\mathrm{Aut}_k(X \otimes_k K)$. This is just a computational check:

$$a_s s(a_t) = \phi^{-1} s(\phi) s\left(\phi^{-1} t(\phi)\right) = \phi^{-1} s(\phi) s(\phi^{-1}) st(\phi) = a_{st}.$$

Moreover, the class of $(a_s)_{s \in G}$ in $H^1(G, \mathrm{Aut}_k(X \otimes_k K))$ is independent of the choice of isomorphism ϕ. To see this, suppose that ψ is another isomorphism, and define $b_s = \psi^{-1} s(\psi)$. If we define $\alpha = \phi^{-1}\psi$, then we can check that for all $s \in G$, $\alpha b_s s(\alpha)^{-1} = a_s$. But this means that they represent the same class in $H^1(G, \mathrm{Aut}_k(X \otimes_k K))$. □

The important philosophy is that this natural map is often a bijection.

Lemma 19.6 (Second stage). *Assume that $1 \to C \to B \to A \to 1$ is an exact sequence of G-groups, and that C lies in the center of B. Then there is a natural map $H^1(G, A) \to H^2(G, C)$.*

Proof. Given $[a] \in H^1(G, A)$ let a_s be the 1-cocycle corresponding to it in $C^1(G, A)$. The map $B \to A$ is surjective, so we can lift it to a 1-cocycle $\tilde{a}_s$ in $C^1(G, B)$. Now apply the coboundary map to this to get a 2-cochain

$$c_{s,t} = s(\tilde{a}_t)(\tilde{a}_{st})^{-1}\tilde{a}_s.$$

This takes values in the kernel of $B \to A$, so by exactness we get a 2-cochain from G to C. To check that this is a 2-cocycle, we check that for all $s, t, u \in G$,

$$s c_{t,u} c_{st,u}^{-1} c_{s,tu} c_{s,t}^{-1} = 1$$

where we have to use the crucial fact that C lies in the center of B. We define the image of $[a]$ to be the image $[c]$ in $H^2(G, C)$. It can be checked that this does not depend on the lift of a. □

[*End of the course!*]