Week 5

???

5.1 Wedderburn-Artin Theory

10/23:
- Share notes with Rudenko at the end of the course!
- Today: Wedderburn-Artin theory.
  - Noncommutative algebra.
  - Noncommutative is a big part of math, partially because of its relation to QMech and partially because of its use in math, itself.
  - There is a textbook: Lang (2002). It's a hard, grad-level textbook but very cleanly written. Not a bad book to have in our mind as we start to encounter category theory.
- So here's what were talking about.
  - Our main object is A, an **associative algebra** over a field F.
- Left vs. right algebras.
  - When A is not commutative, we have to specify which we are dealing with.
  - Let A be an algebra over F.
  - Recall left-modules and right-modules.
    - In a left module, you can multiply $A \times M \to M$ where $(ab)m = a(bm)$.
    - In a right module, $(ab)m = b(am)$. More simply, $m(ab) = (ma)b$.
    - With modules, we get submodules, quotient modules, homomorphisms of modules, etc.
  - Let $I \subset A$ be a left-submodule. Thus, it is a subspace of A such that for all $a \in A$, $aI \subset I$, i.e., a left ideal.
  - In a right-submodule $I \subset A$, we have that for all $b \in A$, $Ib \subset I$, i.e., a right ideal.
  - In a two-sided ideal $I \subset A$, we have for all $a, b \in I$ that $aI \subset I$ and $Ib \subset I$.
  - Example: The matrix algebra is the prototypical noncommutative algebra. Consider $M_{2\times 2}(\mathbb{C})$.
    - Pick $v = (1, 0)$.
    - Look at ideal $I = \{X \in M_{2\times 2} \mid Xv = 0\}$. This is called the **annihilator**, and it is a left ideal. Explicitly, this ideal is the subset of all matrices of the form

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$$

      for $a, b \in \mathbb{C}$.

    - An example of a right ideal is all those such that $vX = 0$, i.e., all matrices of the form

$$\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}$$

    - There are *no* two-sided ideals herein, save the trivial one.

- **Simple** (algebra): An algebra for which there are no nontrivial two-sided ideals.
- Every time you go more abstract, it's more boring because you have less things to play with, but we can derive more general rules.
  - We'll only stay so abstract for 2-3 lectures.
- We want to convert left-algebras to right-algebras.
  - To do so, we can construct **opposite algebras**.
- **Opposite algebra** (of A): The algebra with the same vector space structure as A, but with the reversed multiplication such that $a * b$ in this space yields $b * a$ in A. *Denoted by* $\boldsymbol{A}^{\mathbf{op}}$.
  - Left ideals of A become right ideals of A^{op} and vice versa. Two-sided ideals stay the same.
  - In category theory, left-modules over A are equivalent to right-modules over A^{op}.
  - Opposite algebras are briefly defined on Fulton and Harris (2004, p. 308) and are not defined anywhere else in any of the other sources.
- Example: Consider $M_{n\times n}(F)^{\text{op}}$.
  - Claim: This algebra equals regular $M_{n\times n}(F)$.
  - The map between these spaces is $A \mapsto A^T$.
  - There are other maps, such as conjugation and then transpose.
  - Being isomorphic to your opposite is a strange and interesting property!
- Example: $\mathbb{C}[G]^{\text{op}} \cong \mathbb{C}[G]$.
  - Left as an exercise to find the map.
- Let M, N be modules. We now investigate some properties of $\text{Hom}_A(M, N)$, a nice abelian group.
  - Explicitly, it's

$$\text{Hom}_A(M,N) = \{f : M \to N \text{ linear} \mid f(am) = af(m)\ \forall\ a \in A\}$$

  - We have that

$$\text{Hom}_A(M_1 \oplus M_2, N) \cong \text{Hom}_A(M_1, N) \oplus \text{Hom}_A(M_2, N)$$

    - Prove by looking at what happens to vectors of the form $(M_1, 0)$ and $(0, M_2)$.

  - Similarly,

$$\text{Hom}_A(M, N_1 \oplus N_2) \cong \text{Hom}_A(M, N_1) \oplus \text{Hom}_A(M, N_2)$$

- What if we have $\text{Hom}(M_1 \oplus \cdots \oplus M_n, N_1 \oplus \cdots \oplus N_m)$?
  - Then we have by induction from the previous cases that

$$\text{Hom}(M_1 \oplus \cdots \oplus M_n, N_1 \oplus \cdots \oplus N_m) = \bigoplus_{\substack{i=1,\dots,n \\ j=1,\dots,m}} \text{Hom}(M_i, N_j)$$

  - Let $\varphi_{ij} \in \text{Hom}(M_i, N_j)$.

- At this point, it's very natural to write matrices

$$\begin{array}{cc} & n \\ m & \begin{bmatrix} & & \\ & \varphi_{ji} & \\ & & \end{bmatrix} \end{array} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} \varphi_{11}(m_1) + \cdots + \varphi_{1n}(m_n) \\ \vdots \\ \end{pmatrix} = \begin{pmatrix} (\varphi(m)) \\ \vdots \\ \end{pmatrix}$$

  - Is it ϕ_{ji} or ϕ_{ij}?? Lang (2002, p. 642) seems to back the latter.

- To make this make sense for ourselves, write out the 2×2 case from $M_1 \oplus M_2 \to M_1 \oplus M_2$.

$$\begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = \begin{pmatrix} \\ \end{pmatrix}$$

- Matrices made out of maps can seem really confusing when you first start, but in time, it will make sense.

- Recall the result from last time about division algebras.
- The main object we need to understand is a **semisimple algebra**.
- **Semisimple** (module): A module that satisfies any of the conditions in the following theorem.
  - Note that we proved something analogous to condition 3 early on! This was the complements theorem.
  - This is equivalent for infinite-dimensional algebras; we need **Zorn's lemma** regarding maximal ideals/the axiom of choice here, though.
- Theorem: Let A be an algebra over F, and let M be a left-module. Then TFAE.
  1. $M = \bigoplus_{i \in I} S_i$, where each S_i is a simple module and I is an **indexing set**, not a simple module/ideal.
  2. $M = \sum_{i \in I} S_i$, where the sum is *not* direct.
  3. For all submodules $N \subset M$, there exists N' such that $M = N \oplus N'$.

  Proof. This proof only applies for the case that M is finite dimensional; the theorem is more general than that, but we are not interested in the more general case.

  ($1 \Rightarrow 2$): Very clear; all direct sums are sums.

  ($2 \Rightarrow 1$): Consider the maximal subset $J \subset I$ (by inclusion, not by indices) of our indexing set such that

$$\sum_{i \in J} S_i = \bigoplus_{i \in J} S_i$$

  In other words, J induces the highest-dimension sum of submodules that is a direct sum. Note that we can still find a singleton J in the direct-sum-of-one-thing case, so we're starting from a good base case.

  Claim: $\bigoplus_{i \in J} S_i = M$. Suppose not. Then there exists $m \in M$ such that $m \notin \bigoplus_{i \in J} S_i$ and $m = s_{i_1} + \cdots + s_{i_k}$ where each $s_{i_j} \in S_{i_j}$. If all $s_{i_1}, \dots, s_{i_k} \in \bigoplus_{i \in J} S_i$, then we have arrived at a contradiction and we are done. If not, then there exists some s_{i_t} such that $s_{i_t} \notin \bigoplus_{i \in J} S_i$. Now consider $S_{i_t} \cap (\bigoplus_{i \in J} S_i)$. This will be a submodule of S_{i_t}. But since S_{i_t} is simple by hypothesis, this means that $S_{i_t} \cap (\bigoplus_{i \in J} S_i)$ either equals S_{i_t} or 0. However, we know that it can't equal S_{i_t} because above, we found $s_{i_t} \in S_{i_t}$ such that $s_{i_t} \notin \bigoplus_{i \in J} S_i$. Thus, $S_{i_t} \cap (\bigoplus_{i \in J} S_i) = 0$. But this means that $S_{i_t} + \bigoplus_{i \in J} S_i$ is a direct sum, which contradicts the choice of J as maximal.

  ($1 \Rightarrow 3$): Let's take a submodule $N \subset M$. By 1, $M = \bigoplus_{i \in I} S_i$. Let's look a tall subsets J such that

$$N + \sum_{j \in J} S_j = N \oplus \left(\sum S_j \right)$$

Look at the maximal one by inclusion. Then once again, by the same proof strategy as above,

$$N \oplus \underbrace{\left(\sum S_j\right)}_{N'} = M$$

($3 \Rightarrow 1$): We use what we've learned about representations. Let $M = N_1 \oplus N_2$. Then N_2, if nonsimple, has subsets $N_2 \oplus N_3$. We can continue on and on. Because dimensions finitely decrease, we'll eventually have to arrive at a sum $N_1 \oplus \cdots \oplus N_m$ of simples. ☐

- Now, we have 3 definitions of semisimple modules.
- Corollary: If A is an algebra, M is a semisimple module, and $N \subset M$ is a submodule, then...
  1. N is semisimple.

     Proof. Let L be a submodule of N. We need to find a complement of L inside N. We can find $L' \subset M$ such that $L \oplus L' = M$. Then $L' \cap N \subset N$ is the complement of L in N. Why? Because of the following.
     Claim: $(L' \cap N) \bigoplus L = N$. Not intersecting: $L' \cap N \cap L \subset L' \cap L = 0$. Summing to the whole thing: Let $n \in N$ be arbitrary. Then since $n \in M$, there exists $\ell, \ell' \in L, L'$ such that $n = \ell + \ell'$. But since $n, \ell \in N$, we must have $\ell' \in N$ as well. Therefore, $\ell' \in L' \cap N$. ☐
  2. M/N is semisimple.
- Takeaway: Submodules and quotient modules of semisimple modules are semisimple modules.
- Lang (2002) has a write-up of the proof from today's class.
  - Funnily enough, it is the only textbook that does! Fulton and Harris (2004) doesn't have it; not even Etingof et al. (2011) has it!

5.2 Semisimple Algebras

10/25:
- More associative algebra today; we'll wrap it up next time.
- Review.
  - Let A be a finite dimensional associative algebra over a field F.
  - We want to understand when this algebra is very close to a *group algebra*.
    - Recall that $A = F[G] = \{a_{g_1}g_1 + \cdots + a_{g_n}g_n \mid a_i \in F\}$ is the group algebra of G a finite group.
  - Recall left modules.
    - These are very similar to representations.
    - Indeed, if we have a left module M, then we have a multiplication map $\rho : A \times M \to M$ with properties such as associativity, etc.
  - Recall right modules.
    - In a group representation, left modules over A are essentially the same thing as right modules over A^{op}.
    - Because there is a bijection between left modules over A and right modules over A^{op}, we sometimes have the case where the thing doesn't change??
  - All of the above motivated the definition of *semisimple*: If A is a finite dimensional algebra and M is a finite-dimensional module, then M is *semisimple* if it satisfies any one of three conditions from last time's theorem.

    - Note: When we describe a module as "finite-dimensional," we mean this in the sense of a vector space, i.e., literally finite-dimensional as opposed to finitely generated or anything like that.
    - Note: "Last time's theorem" refers to the semisimplicity conditions one, which is a part of Wedderburn-Artin theory but is *not* the **Wedderburn-Artin *theorem***. We'll get to this theorem eventually, but that's still in the future.

- Theorem (Maschke's theorem): Let G be a finite group and let F be a field. Suppose $(|G|, \operatorname{char} F) = 1$, i.e., they are coprime. Then every finite-dimensional left module over $F[G]$ is semisimple.

  Proof. We've already basically done this proof as part of last time's theorem. Here's a refresher, though.

  Let M be an arbitrary finite-dimensional left module over $F[G]$. Then there exists a map $F[G] \to \operatorname{End}_{F[G]}(M)$, or $G \to GL(M)$. Thus, M is a G-representation, which satisfies condition (3) from last time's theorem because of the complements theorem, stated as Theorem 1 from Serre (1977) for instance. $\square$

- Takeaway: The proof actually works for any field under this condition.
  - Rudenko will reprove Maschke's theorem tomorrow a different way.
- In an algebra, we have a multiplication map $\cdot : A \times A \to A$.
  - If we take the perspective that this map defines an action of the left A on the right one, we see that A has the structure of a left A-module.
  - Vice versa for right-modules.
- **Semisimple** (algebra): An algebra for which every finite-dimensional A-module is semisimple. *Also known as* **semi-simple**.
- Theorem: Let A be a finite-dimensional associative algebra. Then TFAE.
  1. A is a semisimple algebra.
  2. A is semisimple as a left-module over A. Equivalently, as an A-module, $A \cong S_1^{n_1} \oplus \cdots \oplus S_k^{n_k}$.
  3. (Wedderburn-Artin theorem) $A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$, where the $D_1, \dots, D_k$ are division algebras. Note that the isomorphism is an isomorphism of algebras.
- We will prove this theorem in just a moment, but there are a few preliminary comments to be made first.
- Let's look at the algebra $\mathbb{H}$.
  - We can create matrices of quaternions, and we can add and multiply these matrices just fine.
  - However, the determinant is weirder: Is it $ad - bc$ or $ad - cb$?
    - There is a theory of determinants of noncommutative fields called **algebraic *k*-theory**, but we will not get into that.
- Example: Proving (3) for $\mathbb{C}[G]$.
  - We have $\mathbb{C}[G]$. There are not many division algebras over complex numbers; only one, in fact: Complex numbers.
  - Let $V_1, \dots, V_k$ be the irreps. Then we want to show that

$$\mathbb{C}[G] \cong M_{d_1}(\mathbb{C}) \oplus \cdots \oplus M_{d_k}(\mathbb{C})$$

    where $d_i = \deg V_i$.

- Note: Matrices give us a nice way to compute otherwise complicated elements of $\mathbb{C}[G]$.
- Proof: Define a map $F : \mathbb{C}[G] \to M_{d_1}(\mathbb{C}) \oplus \cdots \oplus M_{d_k}(\mathbb{C})$ by

$$x \mapsto (\rho_{V_1}(x), \dots, \rho_{V_k}(x))$$

  - F is injective: $F(x) = 0$ implies that $\rho_{V_i}(x) = 0$ $(i = 1, \dots, k)$, so $xV_i = 0$ $(i = 1, \dots, k)$. In particular, this means that $x = x \cdot 1 = 0$.
  - F is surjective: F is injective and $\dim(\mathbb{C}[G]) = \sum d_i^2 = \dim[M_{d_1}(\mathbb{C}) \oplus \cdots \oplus M_{d_k}(\mathbb{C})]$.
  - F is a homomorphism of algebras: Left as an exercise.
- Note: Remember this theorem very well because it allows you to treat group rings very easily.
- Tomorrow, we'll bring characters into this picture.

- We now state a lemma that will be used to prove $2 \Rightarrow 3$.
- Lemma: Let $\text{End}_A(A)$ denote the set of A-module endomorphisms of A. Then

$$\text{End}_A(A) \cong A^{\text{op}}$$

as algebras.

Proof. To prove the claim, it will suffice to construct an A-algebra isomorphism $F : \text{End}_A(A) \to A^{\text{op}}$. Define F by

$$F(f) := f(1)$$

for all $f \in \text{End}_A(A)$. It should be fairly clear that

$$F(f + g) = F(f) + F(g) \qquad\qquad F(1) = 1$$

Proving that $F(f \circ g) = F(f) * F(g)$ is slightly more involved, but can be done as follows.

$$F(f \circ g) = [f \circ g](1) = f(g(1)) = f(g(1) \cdot 1) = g(1) \cdot f(1) = F(g) \cdot F(f) = F(f) * F(g)$$

Lastly, by plugging $f = a = aI$ and $g = f$ into the above, we can recover

$$F(af) = a * F(f)$$

Thus, F is an A-algebra *homomorphism.* To prove that it is an *isomorphism*, consider the inverse map $G : x \mapsto [a \mapsto ax]$. We can show that $F \circ G = 1_{A^{\text{op}}}$ and $G \circ F = 1_{\text{End}_A(A)}$, thus completing the proof. ☐

- We now prove the above theorem, which we restate for simplicity.
- Theorem: Let A be a finite-dimensional associative algebra over F. Then TFAE.
  1. A is a semisimple algebra.
  2. A is semisimple as a left-module over A. Equivalently, as an A-module, $A \cong S_1^{n_1} \oplus \cdots \oplus S_k^{n_k}$.
  3. (Wedderburn-Artin theorem) $A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$, where the $D_1, \dots, D_k$ are division algebras. Note that the isomorphism is an isomorphism of algebras.

Proof. One line; very simple, but a little weird conceptually.

($2 \Rightarrow 1$): To prove that A is a semisimple algebra, it will suffice to show that every finite-dimensional A-module over F is semisimple. Let $M = Fe_1 + \cdots + Fe_n$ be an arbitrary finite-dimensional A-module. To show that it's semisimple, it will suffice to demonstrate that it's equal to the direct sum of simple modules. Define a map $A^n \to M$ by

$$(a_1, \dots, a_n) \mapsto a_1e_1 + \cdots + a_ne_n$$

This should (fairly clearly) be a surjective homomorphism of left-modules (how do we know that all $a_i \in F$??). Moreover, since $A = S_1 \oplus \cdots \oplus S_k$ is semisimple as a left A-module by hypothesis, we have that $A^n = S_1^n \oplus \cdots \oplus S_k^n$ (how does this imply that M is equal to the direct sum of simple modules??).

($3 \Rightarrow 2$): Work it out in the HW!

($2 \Rightarrow 3$): Let's take $A = S_1^{n_1} \oplus \cdots \oplus S_k^{n_k}$ a left A-module where each S_i is simple. Then by the lemma,

$$A^{\text{op}} \cong \text{End}_A(A) = \text{Hom}_A(A, A) = \text{Hom}_A(S_1^{n_1} \oplus \cdots \oplus S_k^{n_k}, S_1^{n_1} \oplus \cdots \oplus S_k^{n_k}) = \bigoplus_{i,j=1}^{k} \text{Hom}_A(S_i^{n_i}, S_j^{n_j})$$

By Schur's lemma for associative algebras,

$$\text{Hom}_A(S_i, S_j) = \begin{cases} 0 & i \neq j \\ D_i & i = j \end{cases}$$

where each D_i is a division algebra. Thus, continuing from the above,

$$A^{\text{op}} \cong \bigoplus_{i=1}^{k} \text{Hom}_A(S_i^{n_i}, S_i^{n_i}) = \bigoplus_{i=1}^{k} M_{n_i}(\text{Hom}_A(S_i, S_i)) = \bigoplus_{i=1}^{k} M_{n_i}(D_i)$$

$\square$

- Consequence: It follows because the D_i's are division algebras that

$$A \cong \bigoplus_{i=1}^{k} M_{n_i}(D_i^{\text{op}})$$

  - What was the point of this??
- Note from last time that we forgot to discuss: A quotient module of a semisimple module is semisimple. Proving this will be in the next HW.
- **Radical** (of A): The finite dimensional A-algebra defined as follows. *Also known as* **Jacobson ideal**, **Jacobson radical**. *Denoted by* $\mathbf{Rad(A)}$. *Given by*

$$\text{Rad}(A) = \{a \in A \mid aS = 0 \text{ for any simple module } S\} \subset A$$

  - Immediate fact: $\text{Rad}(A)$ is a two-sided ideal.
  - This is because...
    - $x \in A$ and $a \in \text{Rad}(A) \implies (xa)S = x(aS) = x(0) = 0 \implies xa \in \text{Rad}(A)$;
    - $x \in A$ and $a \in \text{Rad}(A) \implies (ax)S = a(xS) = 0 \implies ax \in \text{Rad}(A)$.
  - Note that xS is simple in the above line because a scaled simple module is still simple.
- Theorem: A is semisimple iff $\text{Rad}(A) = 0$.
  - This will be explained next time.
  - In other words, if there are problematic elements, the algebra is not semisimple.
  - Quotienting algebras by two-sided ideals gives algebras, so if A is not semisimple, we know that $A/\text{Rad}(A)$ *is* semisimple!
- This week: A brief primer on noncommutative algebra that is probably worth studying for the midterm.
- Next week: Number theoretic stuff, integer elements, groups, etc.
- Most people/books don't treat the finite-dimensional case here (so it's not written up anywhere) because they view it as too restrictive; instead, they prefer to use the **Artinian** condition.