Theory of Semisimple Rings: Summer 2018 REU

Professor Richard Elman

Anish Chedalavada

1 Central Simple Algebras

In this section the theory of semisimple rings is applied to the concept of finite F-dimensional simple algebras that contain a field F as their center. In particular, as these rings are simple and left artinian, they are isomorphic to matrix rings over division rings. We use this fact to prove important results such as the Double Centralizer Theorem, which is later used to classify the fields over which a division algebra is split; the Skolem-Noether Theorem, which classifies all automorphisms of a central simple algebra and the conjugacy classes of simple subalgebras in addition to proving Wedderburn's Theorem on finite division rings, and classify the reduced characteristic polynomial, an invariant which we use to prove Tsen's theorem.

Exercise 1.1. *Let D be a division F -algebra with char $F = p > 0$. Let $a \in D \setminus F$ satisfy $a^{p^n} = a$ for some positive integer n. Show that there exists an element $x \in D^\times$ satisfying $xax^{-1} = a^i \neq a$ for some i.*

Proof. We have that field F is of characteristic p and thus must contain the prime subfield $\mathbb{Z}_p$. From field theory, we have that there is a unique finite field extension of order p^n such that every element of the field is a rootof $t^{p^n} - t$; i.e. that a must belong to some subfield of this extension. As the polynomial is of degree p^n, these must be all the solutions, and as every root is distinct, the polynomial is separable. In particular, we have that the field extension K/F containing $\mathbb{Z}_{p^n}$ is separable over the base field and that any given root of the polynomial must also be separable. Thus, a is separable over the base field. Furthermore, as every extension K of a finite field is normal (i.e. the splitting field of the polynomial $t^{p^n} - t$ for $n = \dim_{\mathbb{Z}_p} K$ we have that the extension $F(a)$ must in particular be the extension $F(\mathbb{Z}_p(a))$ and thus must also be a normal extension, given that it is a splitting field. Thus, $F(a)$ is a Galois extension of dimension greater than 1, and there is thus a nontrivial Galois group $G(F(a)/F)$. There exists a $\sigma \in G(F(a)/F)$ s.t. $\sigma(a) \neq a$ as the Galois group is nontrivial and must permute the roots of the minimal polynomial, and this yields two distinct F-algebra maps into D given by the inclusion map $\iota : F(a) \hookrightarrow D$ and the Galois transformation $f = \iota \circ \sigma$. By Skolem-Noether, there is a unit $u \in D^\times$ s.t. $ufu^\times = \iota$. The result follows. □

Exercise 1.2. *The F-subalgebras in $M_n(F)$ that are isomorphic to F^n are conjugate to the subalgebra of diagonal matrices.*

Proof. If A is F-split then $A \cong \mathbb{M}_n(F)$, we have the diagonal F-subalgebra B on generators $a_{ii} \mid 1 \leq i \leq n$ where a_{ii} represents the matrix T that is 0 in every entry except in the ii entry, where it is 1. The direct product F^n is an n dimensional F-vector space equipped with coordinate wise multiplication, and thus the generators of the algebra are the basis vectors of the direct product $\{e_1, ..., e_n\}$. Define an F-algebra map by $\phi : F^n \to B$ via $\phi : e_i \mapsto a_{ii}$. For any given diagonal matrix with entries $\{\lambda_1, ..., \lambda_n\}$ we have that the vector $(\lambda_1, ..., \lambda_n)$ maps to it under ϕ. Furthermore, as a_{ii} are linearly independent in $\mathbb{M}_n(F)$ and e_i is not mapped to zero for any e_i, the map ϕ must be injective as F is a field. So ϕ is an isomorphism. By the Skolem-Noether Theorem, if there is another algebra isomorphic to F_n it is isomorphic to the subalgebra of diagonal matrices and thus conjugate to the subalgebra of diagonal matrices.

□

Exercise 1.3. *Show a finite dimensional central simple F-algebra A of degree n is split if and only if it contains an F-subalgebra isomorphic to the direct product $F^n = F \times ... \times F$.*

Proof. "⇒" Subalgebra of diagonal matrices from the previous problem suffices.
"⇐" Suppose A contains an F-subalgebra B isomorphic to F^n. As A is of degree n, we have that there is a maximal subfield K/F that splits A. As the tensor product takes F-subalgebras to K-subalgebras, we have that

□

2 Brauer Group

This section furthers on the ideas of the Central Simple Algebras section by introducing the notion of a Brauer group, a field invariant that is a group on the set of all Brauer-equivalent central simple F-algebras. The Brauer group is a torsion group, and it is possible to derive which central simple F-algebras are split over some field extension K/F by using the isomorphism of $\mathrm{Br}(K/F)$ to the second cohomology group of the Galois group $G(K/F)$ with coefficients in $L^{(\times)}$. This allows us to derive that the Brauer group is torsion, an application of which we will explore in the exercise below; the proof has been adapted from [1].

3 C_n-fields

This section introduces the concept of a C_n-field, a field such that every homogenous polynomial of degree d in more than d^n variables has a nontrivial zero; i.e. we have that algebraically closed fields are C_0, so on and so forth. The Lang-Nagata and the Lang theorems provide two important classifications about such fields: one, a generalization of the Nullstellensatz to arbitrary C_n-fields, and the facts that all algebraic extensions K/F of a C_n field F are C_n, though $F(t)$ for t and indeterminate is always C_{n+1}. The concept is used to show Tsen's theorem; this chapter deals with a specific case of Tsen's theorem, namely the generalized quaternion algebras.

Exercise 3.1.

4 Introduction to Representation Theory

4.1 Representations

This section serves to present one of the motivations behind classifying semisimple rings. We introduce the idea of a group ring $R[G]$ as an algebra over some ring R or field F, with the algebra multiplication inherited from the group. The group ring thus may have an associated module N that it acts upon using the standard R-multiplication from the ring and some map $\phi : G \to Aut_F N$ such that the G-multiplication acts via the group action on N as an F-module. These maps are called representations. The section goes on to prove Maschke's Theorem, that every group ring over a field $F[G]$ is semisimple, i.e. completely reducible over itself as a module. Thus, every group ring over a field is isomorphic to some product $\mathbb{M}_{n_1}(D_1) \times ... \times \mathbb{M}_{n_m}(D_m)$ unique up to order via the Artin-Wedderburn theorem. This yields several maps from the group into matrix rings over division rings, which can be restricted to maps $\phi_i : G \to GL_{n_i}(D_i)$. These maps are the representations of G into some $Aut_F N$.

Lemma 4.1. *Let A be a semisimple F-algebra with basic set $\{\mathfrak{A}_i, ..., \mathfrak{A}_m\}$. If M is a nonzero irreducible A-module, then $M \cong \mathfrak{A}_i$ as an A-module for some $1 \leq i \leq r$. Let $m \in M$.*

Proof. By the universal property of free modules, we have an A-module map $\psi : A \to M$ via $1_A \mapsto v$. As an A-module, being semisimple, we have that $A = \coprod_{i=1}^{r} \mathfrak{A}_i^{n_i}$. Given that M is irreducible and contains no proper submodules, and clearly ψ is not the zero map, we must have that $\psi(A) = M$. However, ψ is an A-module map and thus must commute with coproduct. This means that

$$\psi(A) = \psi\left(\coprod_{i=1}^{r} \mathfrak{A}_i^{n_i}\right) = \bigoplus_{i=1}^{r} \psi(\mathfrak{A}_i)^{n_i} = M$$

As M is irreducible, it contains no proper submodules, and thus there exists some unique $\mathfrak{A}_i^{(k)}$ s.t. $\psi(\mathfrak{A}_i^{(k)}) = M$. Furthermore, as every element of the basic set is a minimal left ideal, it must be an irreducible left A-submodule and contains no proper submodules, i.e. no kernels. Thus, $\psi|_{\mathfrak{A}_i^{(k)}}$ is an isomorphism, and we have the claim. □

Exercise 4.1. *Show that for F an algebraically closed field of characteristic zero, G a finite group, z an element of the center of $F[G]$, V an irreducible $F[G]$-module, there exists an element λ in F satisfying $zv = \lambda v$ for all $v \in V$.*

Proof. We have that F is algebraically closed of characteristic zero. Thus, Maschke's theorem applies, and as F is algebraically closed, we have that $F[G]$ must be F-split. We thus have

$$F[G] \cong \prod_{i=1}^{r} \mathbb{M}_{n_i}(F)$$

as rings and F-algebras. Moreover, this isomorphism occurs via the left regular representation of $F[G]$ on itself. We will view this isomorphism as equality. We have from the lemma above that any irreducible module of $F[G]$ must be isomorphic to some column space of a simple component of $F[G]$ as an $F[G]$ module; it is the clear that there is a ring homomorphism. However, the center of $F[G]$ is an F-vector space on basis $\{I_1, ..., I_r\}$ for $1 \leq i \leq r$ the corresponding simple component. Thus, we have if $z \in Z(F[G])$, then $z = (\lambda_1 I_1, ..., \lambda_r I_r$. Let $\mathfrak{A}_i$ be some column space of $\mathbb{M}_{n_i}(F)$. Let $v \in \mathfrak{A}_i$ be arbitrary. Then $z(0, ..., v, ..., 0) = (0, ..., \lambda_i v, ..., 0)$. The result follows. □

5 Split Group Rings

This section introduces Jacobson's Density Theorem for irreducible R-modules, i.e. that for $\lambda : R \to End_{End_R(M)}(M)$, Im$\lambda$ acts densely on M as an $\text{End}_R(M)$ module (vector space, as it is a division ring by Schur's Lemma). This leads into Burnside's Theorem on irreducible modules over F-algebras, which the following exercises make use of to formalise the conditions for which an algebra is F-split.

Exercise 5.1. *Let F be a field, A an F-algebra (not necessarily finitely generated), and M a completely reducible A-module. Show if $End_A(M) \cong F$ then M is an irreducible A-module.*

Proof. As M is a completely reducible A-module then $M = \coprod_I M_i$ for $M_{i\in I}$ irreducible A-modules. Fix $j \in I$ s.t. $M_j \neq 0$, there exists an A endomorphism $\sigma : M \to M$ s.t. $sigma|_{M_j} = Id_{M_j}$ and is zero everywhere else. σ is clearly a well defined endomorphism as the submodules in the direct sum are pairwise disjoint. However, σ cannot contain a kernel as by assumption every A endomorphism is invertible. Thus, $I = \{j\}$ and M is irreducible. □

It is important to note that the above proof generalizes to any arbitrary division ring.

Exercise 5.2. *Let F be a field, A a semi-simple finite dimensional F -algebra. Then A is F-split $\iff$ $F \cong End_A(M)$ for every irreducible A-module M. In particularly, if F is algebraically closed, then A is F-split.*

Proof. We have that A is a semisimple finite dimensional F-algebra, and thus $A \cong \mathbb{M}_{n_1}(D_1) \times ... \times \mathbb{M}_{n_m}(D_m)$ for some division rings $D_1, ..., D_m$. Let $\{\mathfrak{A}_1, ..., \mathfrak{A}_r\}$ be a basic set for A, representing all possible irreducible A-modules.

"$\Leftarrow$" By Burnside's Theorem, $\text{End}_A(M) = F \implies L_A(M) = \text{End}_F(M) = \mathbb{M}_n(F)$ for $n = \dim_F M$. Furthermore, we note that $M \cong \mathfrak{A}_i$ for some column space of A. If A were not F-split, then we have some decomposition of $A \cong \mathbb{M}_{n_1}(D_1) \times ... \times \mathbb{M}_{n_m}(D_m)$. Fix $1 \leq i \leq r$. A being the product ring described above, the action of A on any column space of $\mathbb{M}_{n_i}(D_i)$ via left multiplication can be described by $M_{n_i}(D_i)$. As A is an F-algebra, we have that every matrix in A must commute with F. Thus, under $\lambda : A \to \text{End}_F(M)$ via $\lambda : a \mapsto (\lambda_a : v \to av)$ we have $\lambda(A) = \mathbb{M}_{n_i}(D_i)$. However, from above, we have that $L_A(M) = \mathbb{M}_n(F)$. Thus, $\mathbb{M}_n(D) \cong \mathbb{M}_n(F)$ for D a division ring with F in its center $\implies D \cong F$. Without loss of generality, this applies to all division rings D_i in the decomposition of A, and thus A must be F-split.

"$\Rightarrow$" If A is F-split, we have that $A \cong \mathbb{M}_{n_1}(F) \times ... \times \mathbb{M}_{n_r}(F)$. $M = \mathfrak{A}_i$ represents some column space of $\mathbb{M}_{n_i}(F)$ and is thus an n_i dimensional vector space over F. Thus, $\text{End}_F(M) \cong \mathbb{M}_{n_i}(F)$ any A-endomorphism must be left multiplication by matrix in $\text{End}_F(M)$ that commutes with every element of A. However, the center of $\mathbb{M}_{n_i}(F)$ is a one-dimensional F-vector space on the basis I. The result follows.

In particular, as there cannot exist any nontrivial division F-algebras for F algebraically closed, $\text{End}_A(M) = F$ for M irreducible A-modules; i.e. A must by F-split for F algebraically closed. □

6 Characters

This section introduces the notion of the character function, given by the trace of the image of a group element under a given representation. The character function has the advantage of being basis invariant and K-linear as a result, and in the section it is shown that the character function completely determines the group representation and the module up to isomorphism.

Exercise 6.1. *Let G be a finite group and F be a field of positive characteristic p, and G a p-group. Suppose that $\psi : G \to GL_n(F)$ is an irreducible representation, show that ψ is the trivial representation.*

Proof. Let $\psi : G \to GL_n(F)$ be an irreducible representation. We have that as G is a p-group, there is an element a in the center of order p. Thus, this element is a root of $t^p - 1 = (t-1)^p$. Thus, under the representation ψ we have $\psi(a)$ contains 1 as an eigenvalue, and thus there is at least one invariant subspace fixed by a, implying there is a basis where 1 lies on the diagonal of $\psi(a)$. As a is in the center of $F[G]$ (in the center pf G) and ψ is an irreducible representation we have that $\psi(a)$ must be a diagonal matrix with all entries equal. However, as there is a basis where 1 lies on the diagonal, this must mean all entries are 1 and thus $a \in ker(\psi)$. Thus, the irreducible representation ψ has a in its kernel and can thus be restricted to an irreducible representation $\widetilde{\psi} : G/ < a > \to GL_n(F)$. As $G/ < a >$ is another p-group, we have another nontrivial kernel and by induction we have that $G \subset ker\psi$. This yields that ψ must be the trivial representation into F. □

7 Orthogonality Relations

One of the motivations behind character theory is to find an F-linear map on semisimple algebras that is basis invariant for a given representation: these are called class functions, and provide another mechanism for analysis of F-algebras, as they furthermore have the property of being multiplicative over the tensor product. These functions are useful as they provide conjugation-invariant (and therefore basis invariant) mechanisms to characterise elements of the algebra spanned by the group, as we will see in the exercises below. In the last section, it was shown that the character completely determines the module up to isomorphism. In this section, character theory is further developed via development of an inner product and orthogonality relations, including the orthogonality of irreducible characters.

Exercise 7.1. *Let G be a finite group. Suppose that char F is zero or does not divide the order of G and $F[G]$ is F-split. Let $\mathfrak{A}$ be an irreducible $F[G]$-module and $B_{\mathfrak{A}}$ the simple component corresponding to $\mathfrak{A}$ corresponding to $\mathfrak{A}$. Then show the unit $f = 1_{B_{\mathfrak{A}}}$ of $B_{\mathfrak{A}}$ satisfies*

$$f = \frac{\chi_{\mathfrak{A}}(1)}{|G|} \sum_G \chi_{\mathfrak{A}}(x^{-1})x$$

Proof. We may assume that G is not the trivial group. From the previous chapter, we have that the unit $f = 1_{B_{\mathfrak{A}}}$ is an idempotent of the ring and is represented by a projection onto the simple component corresponding to $B_{\mathfrak{A}}$. Thus, $f \in Z(F[G])$ and satisfies the following:

$$\chi_{\mathfrak{A}_i}(f) = \begin{cases} 0 & \mathfrak{A}_i \ncong \mathfrak{A} \\ \chi_{\mathfrak{A}}(1) & \mathfrak{A}_i \cong \mathfrak{A} \end{cases}$$

These two properties uniquely characterize f, as if $f \in Z(F[G])$ then $f = \mu_i I_{\mathfrak{A}_i}$, $\mu_i \in F$ for every irreducible module. If the trace is 0 then $\mu_i = 0$ and if it is $\dim_F \mathfrak{A} = \chi_{\mathfrak{A}}(1)$ then by the logic of the last chapter it must be the identity.
Furthermore, as f is an element of the algebra $F[G]$, f can be represented as some sum $f = \lambda \sum_G \alpha(x)x$ with $\alpha : G \to F$ some coefficient function and $\lambda \in F$ some constant. We furthermore have that for any $\sigma \in G$, $\sigma\alpha(x)x\sigma^{-1} = \alpha(\sigma x\sigma^{-1})\sigma x\sigma^{-1}$ as $f \in Z(F[G])$ and thus the sum must be also be conjugation invariant. Thus, α is a class function, and from the lemma and properties above we have that α must be some class function that is orthogonal (by F-linearity of trace) to every irreducible character that is not $\chi_{\mathfrak{A}}$. The most natural choice, of course, is $\chi_{\mathfrak{A}}(x^{-1})$. We may determine λ via:

$$\begin{aligned} \chi_{\mathfrak{A}}(f) = \lambda \sum_G \chi_{\mathfrak{A}}(x^{-1})\chi_{\mathfrak{A}}(x) &\implies \chi_{\mathfrak{A}}(f) = \lambda \sum_G \chi_{\mathfrak{A}}(x^{-1})\chi_{\mathfrak{A}}(x) \\ &\implies \chi_{\mathfrak{A}}(1) = \lambda|G| \\ &\implies \lambda = \frac{\chi_{\mathfrak{A}}(1)}{|G|} \end{aligned}$$

The result follows. □

8 Schur's Theorem

This section provides a generalization to one of the applications of Frobenius's arithmetic lemma, namely that for F a field of characteristic zero G a finite group, $F[G]$ being F-split , the F-dimension of an irreducible $F[G]$-module divides the index of G over its center. The proof makes use of the concept of absolutely irreducible modules $F[G]$ and the fact their F-tensor products remain absolutely irreducible under the diagonal action. This idea will be explored further in the exercises below:

Exercise 8.1. *Show that an irreducible $F[G]$-module V, finite dimensional as an F-vector space, is absolutely irreducible if and only if $End_{F[G]}(V) = F$.*

Proof. "$\Rightarrow$"
"$\Leftarrow$" Applying Burnside's lemma on irreducible modules over F-algebras, we have that if $F = \mathrm{End}_{F[G]}(V)$ then $L_{F[G]}(M) = \mathrm{End}_F(M)$. In particular, $L_{F[G]}(M) = \mathbb{M}_n(F)$. Under the tensor product with the algebraic closure $\widetilde{F}$, we have that a dimension n F-vector space is sent to a dimension n $\widetilde{F}$-vector space, and that $\widetilde{F} \otimes_F F[G] = \widetilde{F}[G]$. We furthermore have that $L_{\widetilde{F}[G]}(M) = \widetilde{F} \otimes_F \mathbb{M}_n(F) = \mathbb{M}_n(\widetilde{F})$. Thus, given any two arbitrary vectors $m, n \in \widetilde{F} \otimes M$, we have an $a \in \widetilde{F}[G]$ s.t. $am = n$ (as image of $\widetilde{F}[G]$ under left multiplication is all endomorphisms of $\widetilde{F} \otimes_F M$. Thus, M is a absolutely irreducible. $\square$

References

[1] Eduardo Tengan. Central Simple Algebras and the Brauer group. In *XVII Latin American Algebra Colloquium*, 2009.