Algebra Qualifying Exam Study Guide

Ariana Chin, Stepan Malkov, Tomoki Oda, Daniel Rui, Victoria Quijano, et al.

Last Updated: January 2026

The following is a collection of notes and exercises intended to help prepare for the UCLA Algebra Qualifying Exam. The content is split into major course topics, including Category Theory, Commutative Algebra, Galois/Field Theory, Group Theory, Representation Theory, and Ring & Module Theory. There may be a number of typos, which generally should not affect the correctness of the arguments herein.

Contents

1 Category Theory

1.1 Equivalences of Categories

Definition 1.1.1. Category C and D is equivalent if there exist a functor $F : C \to D$ and $G : D \to C$ such that two natural isomorphism $\epsilon : FG \to 1_D$ and $\eta : 1_C \to GF$ exist.

An alternative equivalent definition of the categorical equivalence.

Definition 1.1.2. A functor $F : C \to D$ yields an equivalence of categories if and only if it is simultaneously:
full, i.e. for any two objects c_1 and c_2 of C, the map $Hom_C(c_1, c_2) \to Hom_D(Fc_1, Fc_2)$ induced by F is surjective;
faithful, i.e. for any two objects c_1 and c_2 of C, the map $Hom_C(c_1, c_2) \to Hom_D(Fc_1, Fc_2)$ induced by F is injective; and
essentially surjective (dense), i.e. each object d in D is isomorphic to an object of the form Fc, for c in C.

Theorem 1.1.1. *The two definition given above is equivalence under the axiom of choice.*

Lemma 1.1.1. *Any morphism $f : a \to b$ and fixed isomorphism $a \cong a'$ and $b \cong b'$ determine a unique morphism $f'a' \to b'$*

Proof. This is the diagram chasing □

Proof. First suppose we have F, G, η, ϵ. For any $d \in D$ the component of the natural transformation $\epsilon_d : FGd \cong d$ demonstrate F is essential surjective. Consider the two morphisms

$$c \underset{g}{\overset{f}{\rightrightarrows}} c'$$

inside of the category of C. If $Ff = Fg$ then both f and g define an arrow $c \to c'$ making the diagram

$$\begin{array}{ccc} c & \xrightarrow{\eta_c} & GFc \\ {\scriptstyle f \text{or} g}\downarrow & & \downarrow{\scriptstyle GFf=GFg} \\ c' & \xrightarrow[\eta_{c'}]{} & GFc' \end{array}$$

but by the above lemma, we should have the unique arrow to c and c' so $f = g$. That gives faithfullness. By the symmetry it gives the faithfullness of G as well. Fullness can be proven by taking the morphism $k : Fc \to Fc'$ so that rise a morphism $h : c \to c'$. Then again apply the functor GF so that there is a commutative diagram that h correspond to the Gk and GFh. By the faithfullness of $G, GFh = Gk. \to Gh = k$ so this is essentially surjective.
Conversely, suppose F is a full and faithful and essentially surjective. Using the essentaily surjective

and the axiom of the choice, we can chose for each $d \in D$ an object $Gd \in C$ and an isomorphism $FGd \cong d$. For each $l : d \to d'$ we can construct a commutative diagram

$$\begin{array}{ccc} FGd & \xrightarrow{\epsilon_d} & d \\ \vdots & & \downarrow l \\ FGd' & \xrightarrow[\epsilon_{d'}]{} & d' \end{array}$$

Since F is a full and faithful there exist a unique map $Gd \to Gd'$ with image under F. This define a Gl.
Next two things to prove is show Gl is functorial and construct a natural transforamtion $\eta : 1 \to GF$.. Functoriality can be prove by applying $G(1)$ and two things commute same diagram. Define $\eta : c \to GFc$ by speficying isomorphisms $F\eta_c : Fc \to FGFc$ and define $F\eta_c$ as ϵ_{Fc}^{-1}

□

The first definition is similar to the adjoint/ unit and counit. Indeed adjunction is a weaker version of the categorical equivalence, If F, G is the equivalence $Hom(Fc, d') \cong Hom(GFc, Gd')$ by the full and faithfullness, and this is also equal to $Hom(c, Gd')$ because of the isomorphism. On the other hand when unit is isomorphism then F is a faithful functor.

For using the Morita equivalence, we can see the inclusion is preserved under categorical equivalences. Let $h : c \to c'$ is a monomorphism in C we want to show that $F(h)$ is monic. Let $\eta : GF \cong Id_C$ be any natural isomorphism. Suppose there is a $d \in D$ and $f, g : d \to F(c)$ with $F(h) \circ f = F(h) \circ g$. Then: $\eta_{a'} GF(h) \circ G(f) = \eta_{a'} GF(h) \circ G(g)$.So: $h\eta_a \circ G(f) = h\eta_a \circ G(g)$. Since $h\eta_a$ is monic as a composite of monics) we have $G(f) = G(g)$. Because $G$is a faithful, we have $f = g$ as desired. Thus F(h) is monic.

1.2 Exactness

Let $\mathcal{C}$ be an abelian category, i.e. a category with arbitrary kernels, cokernels, and finite biproducts. A sequence

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

is **exact at** Y if $\operatorname{Im} f \cong \ker(g)$, where $\operatorname{Im} f := \ker(Y \to \operatorname{coker} f)$. A **short exact sequence** is a sequence of the form

$$0 \to X \xrightarrow{f} Y \xrightarrow{g} Z \to 0$$

which exact at X, Y, Z, i.e. $X \cong \ker(g) \cong \operatorname{Im} f$, $Z \cong \operatorname{coker}(f) \cong \operatorname{coim}(g)$. Moreover, f is a mono, and g is an epi. An **exact** sequence is a sequence exact except at the first and last objects.

Definition 1.2.1. A functor F is **additive** if it preserves finite biproducts. A functor F between abelian categories is **exact** if it preserves short exact sequences. A functor is

(a) **left exact** if it preserves the exactness of the first four terms in an exact sequence.

(b) **right exact** if it preserves the exactness of the last four terms in an exact sequence.

Remark 1.2.1. Given (not necessarily abelian) categories $\mathcal{C}, \mathcal{D}$, a functor $F : \mathcal{C} \to \mathcal{D}$ is called **(left/right) exact** if it preserves finite (limits/colimits). Since kernels are equalizers, which are limits, and cokernels are coequalizers, which are colimits, this more general definition implies the definition for abelian categories.

Remark 1.2.2. Contravariant functors flip the direction of the sequence, but the definition of exactness as above still holds.

The following theorem lets us deal concretely with all abelian categories as categories of modules over a ring:

Theorem 1.2.1 (Freyd-Mitchell Theorem)**.** *Let $\mathcal{C}$ be an abelian category. Then, there exists a ring R and a full, faithful, exact functor $F : \mathcal{C} \to R\text{-}Mod$.*

In the following, we deal purely with category R-Mod.

Example 1.2.1. (a) $\mathrm{Hom}_R(A, -)$ and $\mathrm{Hom}_R(-, A)$ are both left exact. A module P is **projective** if $\mathrm{Hom}_R(P, -)$ is exact, and a module I is **injective** if $\mathrm{Hom}_R(-, I)$ is exact.

(b) $- \otimes_R A$ is right exact. A module A is **flat** if $- \otimes_R A$ is exact.

Remark 1.2.3. Since a (left/right) adjoint functor preserves all small (colimits/limits), A (left/right) adjoint is (right/left) exact.

1.3 Representabilty and the Yoneda Lemma

Proposition 1.3.1. *Any covariant representable functor (that is, a functor from some category $\mathcal{C}$ to the category of Sets that is naturally isomorphic to $\mathrm{Hom}_{\mathcal{C}(C,-)}$ for some C) preserves limits. Dually, any contravariant representable functor preserves all colimits.*

Proof. Note that natural isomorphism always preserves the property of preserving limits. After all the limit is only determined up to (unique) isomorphism of cones. The natural isomorphism yields such an isomorphism of cones. So in fact, we may assume that $F = \mathrm{Hom}_{\mathcal{C}(C,-)}$ on the nose.

Now, let (A, λ) be the limit of some functor $H : \mathcal{Z} \to \mathcal{C}$. Then, by functoriality, $(FA, F(\lambda))$ is a cone on $F \circ H$. We prove that is universal. To that end, let (X, μ) be a cone on $F \circ H$. Then we have maps

$$\mu_Z : X \to FHZ = \mathrm{Hom}_{\mathcal{C}}(C, HZ),$$

for all Z. Fix $x \in X$. Then (exercise) $(C, \mu_-(x))$ is a cone on H. Thus we have a unique morphism $\phi_x : C \to L$ satisfying $\lambda_Z \circ \phi_x = \mu_Z(x)$.

Now, define

$$\phi : X \to FA = \mathrm{Hom}_{\mathcal{C}}(C, A) : x \mapsto \phi_x.$$

Of course, we have $F(\lambda_Z) \circ \phi = \mu_Z$ because it holds for all $x \in X$. For the same reason ϕ is unique with this property. □

1.4 Categorical Adjoints and (Co)units

Definition 1.4.1. Let $\mathcal{C}$ and $\mathcal{D}$ be categories and consider functors R and L as follows

$$\begin{array}{ccc} & \mathcal{C} & \\ L \swarrow & & \nwarrow R \\ & \mathcal{D} & \end{array}$$

We say that (L, R) is a pair of adjoint functors, or L is left adjoint to R, or R is right adjoint to L if there exists for every $C \in \mathcal{C}$ and $D \in \mathcal{D}$ an isomorphism

$$\theta_{C,D} : \mathrm{Hom}_{\mathcal{D}}(LC, D) \to \mathrm{Hom}_{\mathcal{C}}(C, RD),$$

that is natural in both arguments C and D. We write $L \dashv R$.

The definition and the following equivalent characterisation are both very useful and used equally often.

Proposition 1.4.1. *Let $\mathcal{C}$ and $\mathcal{D}$ be categories and consider functors R and L as follows*

$$\begin{array}{ccc} & \mathcal{C} & \\ L\big(& & \big)R \\ & \mathcal{D} & \end{array}$$

Then (L, R) is an adjoint pair if and only if there exist natural transformations

$$\eta : 1_{\mathcal{C}} \to RL \text{ 'the unit'}$$
$$\varepsilon : LR \to 1_{\mathcal{D}} \text{ 'the counit'},$$

that satisfy the 'counit-unit relations': for all $C \in \mathcal{C}$ and $D \in \mathcal{D}$ the following diagrams are commutative

$$\begin{array}{ccc} RD & \xrightarrow{\eta_{RD}} & RLRD \\ & \searrow & \downarrow{\scriptstyle R(\varepsilon_D)} \\ & & RD \end{array} \qquad \begin{array}{ccc} LC & \xrightarrow{L(\eta_C)} & LRLC \\ & \searrow & \downarrow{\scriptstyle \varepsilon_{LC}} \\ & & LC \end{array}$$

Any standard reference for category theory like Mac Lane or Leinster contains a proof of this fact so I won't prove it here.

The slogan of the following proposition is 'rights adjoints preserve limits, left adjoints preserve colimits'.

Proposition 1.4.2. *Let $R : \mathcal{D} \to \mathcal{C}$ and $L \dashv R$, i.e. R is right adjoint to L. Then R preserves all limits that exist in $\mathcal{D}$. Likewise L preserves all colimits that exist in $\mathcal{C}$.*

Proof. By duality, it suffices to prove the statement for right adjoints.

Concretely we need to show the following: If (A, λ) is the limit of a functor $F : \mathcal{Z} \to \mathcal{D}$ (where $\mathcal{Z}$ is a small category), then $(RA, R\lambda)$ is the limit of $R \circ F : \mathcal{Z} \to \mathcal{C}$. Here we have used the characterisation of a limit as a universal cone.

By functoriality, $(RA, R\lambda)$ is a cone on $R \circ F$. So it is really universality that requires some work. Let (C, μ) be a cone on $R \circ F$. We must prove that there exists a unique morphism $\psi : C \to RA$ satisfying $\mu_Z = R(\lambda_Z) \circ \psi$ for all $Z \in \mathcal{Z}$.

Note that $(LC, L\mu)$ is a cone on $L \circ R \circ F$, again by functoriality. Let ε denote the counit of the adjunction $L \dashv R$ and define for all $Z \in \mathcal{Z}$

$$\tau_Z : LC \to FZ$$

as the composition

$$LC \xrightarrow{L(\mu_Z)} LRFZ \xrightarrow{\varepsilon_{FZ}} FZ$$

Then we claim that (LC, τ) is a cone on F. This follows from the naturality of ε. We leave it as an exercise.

As (A, λ) is the limit of F, we thus have a unique morphism $\phi : LC \to A$ satisfying $\tau_Z = \lambda_Z \circ \phi$. Now set $\psi = R(\phi) \circ \eta_C$ where η is the unit of the adjunction. Then we have the following string of

equalities

$$\begin{aligned} R\lambda_Z \circ \psi &= R\lambda_Z \circ R\phi \circ \eta_C \\ &= R(\lambda_Z \circ \phi) \circ \eta_C \\ &= R(\tau_Z) \circ \eta_C \\ &= R(\varepsilon_{FZ} \circ L(\mu_Z)) \circ \eta_C \\ &= R(\varepsilon_{FZ}) \circ RL(\mu_Z) \circ \eta_C \\ &= R(\varepsilon_{FZ}) \circ \eta_{RFZ} \circ \mu_Z \qquad \text{naturality of } \eta \\ &= \mu_Z \qquad \text{counit-unit relations .} \end{aligned}$$

Uniqueness of ψ follows from uniqueness of ϕ, as we can follow the argument in opposite direction (creating ϕ out of ψ). □

Remark 1.4.1. You could also write this proof referencing only the transformation θ of the definition of an adjunction, see Leinster. Then the maps involved are less concrete and you would reason more with the 'abstract properties' of θ. In number of words used, the proof becomes a bit shorter but every step is perhaps a bit more involved (compared to the steps in the string of equalities). All in all, it is simply a matter of taste.

Lemma 1.4.1. *Let $\mathcal{A}$ and $\mathcal{B}$ be abelian categories and consider functors $L : \mathcal{A} \to \mathcal{B}$ and $R : \mathcal{B} \to \mathcal{A}$. If $L \dashv R$, then L and R are additive functors. Moreover, R is left exact and L is right exact.*

Proof. Recall that a functor between abelian categories is exact if and only if it preserves finite products, which are the same as finite coproducts in an abelian category. Then the statement follows by using the proposition 1.4.2: R preserve finite products because it is a right adjoint and L preserve finite coproducts because it is a left adjoint.

Since kernels are a special case of equalisers, which are limits, F also preserves all kernels and therefore F is left exact. Likewise, cokernels are coequalisers are colimits, so L preserves these and thus is right exact. □

The slogan for the next proposition is 'an equivalence is an adjunction', though the statement is a bit more subtle.

Proposition 1.4.3. *Let $F : \mathcal{C} \to \mathcal{D}$ be a functor. Suppose that there exists a functor $G : \mathcal{D} \to \mathcal{C}$ and natural isomorphisms $\varepsilon : FG \to 1_{\mathcal{D}}$ and $\eta : 1_{\mathcal{C}} \to GF$. Then we can define a natural isomorphism $\varepsilon' : FG \to 1_{\mathcal{D}}$ so that $F \dashv G$ with unit η and counit ε'.*

Remark 1.4.2. With the definition of an equivalence of categories as in definition 1.1.1, this means that we can always modify the counit (or the unit) to make F and G into a bona fide equivalence. In fact, many references in the literature actually define an equivalence to be an adjunction where the unit and counit are isomorphisms.

Proof. First, note that G is fully faithful. After all, $FG \cong 1_{\mathcal{D}}$, so FG is fully faithful, which implies that F must be full and G must be faithful. Likewise $GF \cong 1_{\mathcal{C}}$ implies that F is faithful and G is full.

Now define $\varepsilon' : FG \to 1_{\mathcal{D}}$ for every D via the equation

$$G(\varepsilon'_D) = \eta^{-1}_{GD}.$$

(this is defines ε' uniquely precisely because G is fully faithful). Then naturality of ϵ' follows from naturality of η and functoriality. We verify that ε' and η satisfy the counit-unit relations. One of them is immediately clear by definition:

$$G(\varepsilon'_D) \circ \eta_{GD} = \eta_{GD}^{-1} \circ \eta_{GD} = id_{GD}.$$

Next,

$$\varepsilon'_{FC} \circ F(\eta_C) = id_{FC} \iff G(\varepsilon'_{FC} \circ F(\eta_C)) = id_{GFC}$$

because G is fully faithful. We see that

$$\begin{aligned} G(\varepsilon'_{FC}) \circ GF(\eta_C)) &= \eta_{GFC}^{-1} \circ GF(\eta_C)) \\ &= \eta_C \circ \eta_C^{-1} = id_{GFC}. \end{aligned}$$

This last step uses naturality of η to get a commutative diagram:

$$\begin{array}{ccc} C & \xrightarrow{\eta_C} & GFC \\ {\scriptstyle \eta_C}\downarrow & & \downarrow{\scriptstyle \eta_{GFC}} \\ GFC & \xrightarrow[GF(\eta_C)]{} & GFGFC \end{array}$$

□

2 Module Theory

2.1 The Structure Theorem for Finitely Generated Modules over PID

2.2 Nakayama's Lemma

Theorem 2.2.1 (Nakayama's Lemma)**.** *Let I be an ideal in R, and M a finitely generated R-module. If $IM = M$, then there exists an $r \in R$ with $r \equiv 1 \pmod{I}$ such that $rM = 0$.*

The above is the acclaimed Nakayama's lemma, however the next 3 theorems are easily attained from this statement, and important in their own right to remember, particularly Theorems 2.2.2 and 2.2.4.

Theorem 2.2.2. *If M is a finitely generated R-module and $J(R)M = M$, where $J(R)$ is the Jacobson radical of R, then $M = 0$.*

Theorem 2.2.3. *If M is a finitely generated R-module, N a submodule of M, and $M = N + J(R)M$, then $M = N$.*

Theorem 2.2.4. *If M is a finitely generated R-module and the images of $m_1, \ldots, m_n \in M$ generate $M/J(R)M$ as an R-module, then $m_1, \ldots, m_n$ also generate M as an R-module.*

3 Galois / Field Theory

3.1 Trace/Norm

Let K/F be a finite field extension, and consider for $\alpha \in K$, consider the left multiplication operator $l_\alpha : K \to K$ as an F-linear map. With respect to some basis of K over F, this induces an algebra homomorphism $K \hookrightarrow M_{[K:F]}(F)$.

Definition 3.1.1. The **trace** of α over a field extension K/F is $\mathrm{Tr}_{K/F}(\alpha) = \mathrm{Tr}(l_\alpha) \in F$, and the **norm** of α is $N_{K/F}(\alpha) = \det(l_\alpha) \in F$.

Remark 3.1.1. Note that trace and norm do not depend on the choice of basis.

Let $\alpha \in K$, and consider the sequence of extensions $K/F(\alpha)/F$. Then, if $\{\alpha^i\}$ is a basis for $F(\alpha)/F$, and $\{\beta_j\}$ is a basis for $K/F(\alpha)$, $\{\alpha^i\beta_j\}$ is a basis for K/F. In particular, $l_\alpha^{K/L}$ is a block diagonal matrix consisting of $[K : F(\alpha)]$ submatrices $l_\alpha^{F(\alpha)/F}$. This leads us to the following conclusion:

Proposition 3.1.1.

$$Tr_{K/F}(\alpha) = [K : F(\alpha)]\, Tr_{F(\alpha)/F}(\alpha)$$

and

$$N_{K/F}(\alpha) = N_{F(\alpha)/F}(\alpha)^{[K:F(\alpha)]}.$$

Proof. In the case $K = F(\alpha)$, the characteristic polynomial of l_α equals the minimal polynomial of α, as they have the same degree and the latter is irreducible over F. The formulas above follow from the block diagonal matrix representation of trace and norm over larger field extensions. □

In particular, this means that it suffices to compute the trace/norm of an element α over the base field F to know its trace/norm over any other field extension.

Definition 3.1.2 (An Equivalent Definition of Trace)**.** The **trace** of α over a field extension K/F is $\mathrm{Tr}_{K/F}(\alpha) = [K : F(\alpha)] \sum_i \sigma_i(\alpha)$, where the summation runs over all roots (counted with multiplicity) of the minimal polynomial m_α.

Proof. From Tower Law (Proposition 3.3), we have

$$\begin{aligned}
\mathrm{Tr}_{K/F}(\alpha) &= \mathrm{Tr}_{F(\alpha)/F} \circ \mathrm{Tr}_{K/F(\alpha)}(\alpha) \\
&= \mathrm{Tr}_{F(\alpha)/F}([K : F(\alpha)] \cdot \alpha) \\
&= [K : F(\alpha)] \cdot \mathrm{Tr}_{F(\alpha)/F}(\alpha) \\
&= [K : F(\alpha)] \sum_i \sigma_i(\alpha)
\end{aligned}$$

The second equality comes from the fact that α is in the base field $F(\alpha)$. The last equality comes from the fact that our extension is now $F(\alpha)$, so the degree of the minimal polynomial is $[F(\alpha) : F]$, equal to the degree of the characteristic polynomial χ_α. So, $m_\alpha = \chi_\alpha$, and the trace is now the sum over all roots of $\chi_\alpha = m_\alpha$. □

Proposition 3.1.2. *If K/F is not separable, $\alpha \in K$, then $Tr_{K/F}(\alpha) = 0$.*

Proof. Either $K/F(\alpha)$ or $F(\alpha)/F$ is not separable, so in particular, all fields have positive characteristic $p > 0$. In the former case, $[K/F(\alpha)]_{insep} > 1$, so it divides p, i.e. $[K : F(\alpha)] = 0$ in $\mathbb{F}_p$, while in the latter, the minimal polynomial for α must have zero coefficient multiplying T^{p^m-1} (otherwise it would be separable), so $\mathrm{Tr}_{F(\alpha)/F}(\alpha) = 0$. □

Proposition 3.1.3 (Tower Law)**.** *For a sequence $L/K/F$ of finite field extensions,*

$$Tr_{L/F}(\alpha) = Tr_{K/F}(Tr_{L/K}(\alpha))$$

and

$$N_{L/F}(\alpha) = N_{K/F}(N_{L/K}(\alpha)).$$

Proof. Complicated. □

Proposition 3.1.4. *If K/F is separable,*

$$Tr_{K/F}(\alpha) = \sum_{\sigma} \sigma(\alpha)$$

and

$$N_{K/F}(\alpha) = \prod_{\sigma} \sigma(\alpha),$$

where σ ranges over the distinct F-embeddings of K into its normal closure $\overline{K}$.

Proof. For $K = F(\alpha)$, each F-embedding of $F(\alpha)$ into its normal closure is sends $\alpha \to \alpha'$, where α' is a Galois conjugate of α, so the claim follows. For general K, note that there are $[K : F(\alpha')] = [K : F(\alpha)]$ such F-embeddings, so the claim follows from Proposition 3.1. □

Problem 3.1.1. Show that a linear combination of square roots of primes is irrational.

Proof. Suppose not. Then, $\sum_{i=1}^{n} a_i\sqrt{p_i} \in \mathbb{Q}$. Note that $\mathrm{Tr}_{\mathbb{Q}(\sqrt{p_i})/\mathbb{Q}}(\sqrt{p_i}) = 0$, so if $K = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$, then by additivity of trace,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\sum_{i=1}^{n} a_i\sqrt{p_i}) = 0.$$

Thus the only possible sum could be zero. Multiplying by $\sqrt{p_i}$, we note that $\sum_{j\neq i} a_j\sqrt{p_jp_i} = -a_ip_i$. Since $\mathrm{Tr}_{\mathbb{Q}(\sqrt{p_ip_j})/\mathbb{Q}}(\sqrt{p_ip_j}) = 0$, by additivity of trace it follows that $a_i = 0$. Thus, a linear combination of square roots of primes cannot be rational. □

Problem 3.1.2. Show that a linear combination of cube roots of primes is irrational.

Proof. Suppose not. Since $\mathrm{Tr}_{\mathbb{Q}(p_i^{\frac{1}{3}})/\mathbb{Q}}(p_i^{\frac{1}{3}}) = 0$, by the same argument as above, the only possible sum could be zero. Multiplying by $p_i^{\frac{2}{3}}$, we note that

$$\sum_{j\neq i} a_j(p_jp_i^2)^{\frac{1}{3}} = -a_ip_i.$$

Since $\mathrm{Tr}_{\mathbb{Q}((p_jp_i^2)^{\frac{1}{3}})/\mathbb{Q}}((p_jp_i^2)^{\frac{1}{3}}) = 0$, $a_i = 0$, and the claim follows. □

Remark 3.1.2. The same argument can be applied to show that a linear combination of n-th roots of primes is irrational.

Problem 3.1.3. Show that $3^{\frac{1}{100}} \notin \mathbb{Q}(2^{\frac{1}{100}})$.

Proof. Suppose not. Then, the two extensions are the same, as they are generated by

irreducible polynomials of the same degree. Then,

$$3^{\frac{1}{100}} = \sum_{i=0}^{99} a_i 2^{\frac{i}{100}}.$$

Since the traces of each nonrational element are 0, it follows that $a_0 = 0$. Then, multiplying by $2^{\frac{100-i}{100}}$, we get the trace is over $\mathbb{Q}(2^{\frac{1}{100}})$ is $100a_i$ on the right and 0 on the left, since $x^{100} - 3 \cdot 2^{100-i}$ is irreducible by Eisenstein. Thus, $a_i = 0$. □

Remark 3.1.3. The same argument shows that for any square free integer a and an integer b relatively prime to a, and any integer $n > 2$, $a^{\frac{1}{n}} \notin \mathbb{Q}(b^{\frac{1}{n}})$.

Problem 3.1.4 (Fall 2023 Problem 2). Let $p.q$ be the distinct prime numbers and consider the number field $K = \mathbb{Q}(\sqrt{p} + \sqrt{q})$. Describe all the subfield of K and inclusion between them.

Proof. We have $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{q})$ are linearly disjoint, means $\mathbb{Q}(\sqrt{p}) \cap \mathbb{Q}(\sqrt{q}) = \mathbb{Q}$, if not, then there is $a, b \in \mathbb{Q}$ with $a\sqrt{p} + b = \sqrt{q}$. Taking square for the both side we made $\sqrt{p}$ is rational. Also $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ is a splitting field this is Galois. By the disjointness, we have the Galois group $\mathbb{Z}/2 \times \mathbb{Z}/2$ there are exactly 3 nontrivial proper subgroup. That has to be correspond into $\mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{q}), \mathbb{Q}(\sqrt{pq})$ that they are disjoint with each other, and $\mathbb{Q}$ are trivial subfield. Claim: $\mathbb{Q}(\sqrt{p} + \sqrt{q}) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.
Clearly we have $\mathbb{Q}(\sqrt{p}, \sqrt{q}) \subset \mathbb{Q}(\sqrt{p}, \sqrt{q})$. On the other hand $\mathbb{Q}(\sqrt{p} + \sqrt{q}) \supset \mathbb{Q}(\sqrt{pq})$. But there should no intermediate field except for $\mathbb{Q}(\sqrt{p}, \sqrt{q})$. So $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = K$(Alternatively we can divide $\frac{p^2 - q^2}{\sqrt{p} + \sqrt{q}} = \sqrt{p} - \sqrt{q}$) □

Let's try to generalize this problem.

Problem 3.1.5. (Variant) If $p_1 \dots p_n, p_{n+1}, p_{n+2}$ are distinct prime, then
1.show $K_n = \mathbb{Q}(\sqrt{p_1} \dots \sqrt{p_n})$ does not contains $\sqrt{p_{n+1}}$
2. $[K_{n+1} : \mathbb{Q}]$=2^n
3. Gal$(K_n/\mathbb{Q})$=$(\mathbb{Z}/2\mathbb{Z})^n$
4. $K_n = \mathbb{Q}(\sum_{i=1}^n \sqrt{p_i})$

Proof. 1. We can show by the induction, K_n does not contain niether $\sqrt{p_{n+1}}$ and $\sqrt{p}_{n+1}p_{n+2}$ the base case was shown in the preceeding problem. Assume it is true for $n-1$ and show for the n. If not, we can write $\sqrt{p_{n+1}} = a + b\sqrt{p_n}$ for $a, b \in K_{n-1}$. Here are few cases
Case1. $b = 0$: In this case, by induction hypothesis it is absurd.
Case2. If $a = 0$ then we have $bp_{n+1} = \sqrt{p_n p + n + 1}$ also contradicing hypothesis.
Case 3. Taking square we have $\sqrt{p_n} \in K_{n-1}$ that is also absurd.
2. Since they are linearly disjoint, apply the Galois tower law $[\mathbb{Q}(\sqrt{p_{n+1}}), \mathbb{Q}] = 2$ to the $[K_{n-1}, \mathbb{Q}] = 2^{n-1}$ again also by induction,we can show this is 2^n
3. Due to the linearly disjointness of $K_n/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{p_{n+1}})$ Galois group should be also the direct product of them. That is $(\mathbb{Z}/2\mathbb{Z})^{n-1} \times \mathbb{Z}/2Z$
4. If $\mathbb{Q}(\sum \sqrt{p_i})$ is a proper subfield of K_n. Let put $s = \sum \sqrt{p_i}$. Let I be a index $I \subset \{1 \dots n\}$.

σ_I is an element of $\mathrm{Gal}(K_n/\mathbb{Q})$ such that fix all of $\sqrt{p_j}, j \notin I$ and $\sqrt{p_i}$ to $-\sqrt{p_i}$ for $i \in I$. If s is belong to the proper subfield of K_n then there is a subgroup $G \leqslant Gal(K_n/Q)$ such that fixes s. However $s - \alpha(s) = 2\sum_{i\in I}\sqrt{p_i}$. Thus $K_n = \mathbb{Q}(s)$. □

Problem 3.1.6. (More generalizations) Let μ_n be the $n-$th root of unity. How to compute the galois group of $\mathbb{Q}(\mu_n)(\sqrt[d_1]{p_1}, \ldots, \sqrt[d_n]{p_n})/\mathbb{Q}(\mu_n)$ where d_i divide n.

3.2 Kummer Theory

Kummer theory is the study of field extensions that adjoin certain roots of unity. The first key result of Kummer theory is Hilbert's Theorem 90.

We begin with an important lemma:

Lemma 3.2.1 (Indepence of Characters)**.** *Distinct characters (i.e. group homomorphisms $\chi : G \to F^\times$ for a group G and a field F) are linearly independent.*

Proof. The lemma follows from induction, as it is immediate for $n = 1$ (since $\chi(1) = 1$), and if the characters are linearly dependent and $\chi_n = \sum_{i=1}^{n-1} a_i\chi_i$, then

$$\sum_{i=1}^{n-1} a_i\chi_n(h)\chi_i(g) = \chi_n(h)\chi_n(g) = \chi_n(hg) = \sum_{i=1}^{n-1} a_i\chi_i(hg) = \sum_{i=1}^{n-1} a_i\chi_i(h)\chi_i(g),$$

implying that $a_i = 0$ for all i and proving the lemma. □

Proposition 3.2.1 (Hilbert Theorem 90)**.** *If K/k is a cyclic extension of degree n with Galois group $G = \langle\sigma\rangle$, then for any $\beta \in L$,*

$$N_{K/k}(\beta) = 1 \iff \exists\alpha \in L, \beta = \frac{\alpha}{\sigma(\alpha)}$$

and

$$Tr_{K/k}(\beta) = 0 \iff \exists\alpha \in L, \beta = \alpha - \sigma(\alpha).$$

Proof. If $\beta = \frac{\alpha}{\sigma(\alpha)}$, then

$$N_{K/k}(\beta) = \left(\prod_{\sigma'\in\mathrm{Gal}(K/k)} \sigma'(\beta)\right)^{[K:k(\beta)]} = \left(\prod_{\sigma'\in\mathrm{Gal}(K/k)} \frac{\sigma'(\alpha)}{\sigma'(\sigma(\alpha))}\right)^{[K:k(\beta)]} = 1,$$

since left multiplication induces a permutation of elements of the Galois group. Conversely, suppose that $N_{K/k}(\beta) = 1$. Likewise,

$$\mathrm{Tr}_{K/k}(\beta) = [K : k(\beta)] \sum_{\sigma'\in\mathrm{Gal}(K/k)} \sigma'(\alpha) - \sigma'(\sigma(\alpha)) = 0.$$

Now, since $\{\sigma^k\}$ are distinct characters on the multiplicative group $k^\times$, if $a_k = \prod_{i=0}^{k} \sigma^i(\beta)$, we conclude that $\sum_{k=0}^{n-1} a_k\sigma^k$ is not identically zero, i.e. there is a y such that

$$\sum_{k=0}^{n-1}\prod_{i=0}^{k} \sigma^i(\beta)\sigma^k(y) = \alpha \neq 0.$$

Applying σ on both sides and using the fact that $N_{K/k}(\beta) = a_n = 1$, it follows that

$$\sigma(\alpha) = \sum_{k=0}^{n-1} \left(\prod_{i=0}^{k} \sigma^{i+1}(\beta) \right) \sigma^{k+1}(y) = \sum_{k=0}^{n-1} \left(\frac{1}{\beta} \prod_{i=0}^{k} \sigma^{i}(\beta) \right) \sigma^{k}(y) = \frac{\alpha}{\beta},$$

and the claim follows. Likewise, there is an $\alpha \in L$ such that if $b_k = \sum_{i=0}^{k} \sigma^i(\beta)$, $\sum_{k=0}^{n-1} b_k \sigma^k$ is not identically zero, so by the same argument, for some y such that

$$\sum_{k=0}^{n-1} b_k \sigma^k(y) = \alpha \neq 0,$$

one has

$$\sigma(\alpha) = \sum_{k=0}^{n-1} \left(\sum_{i=0}^{k} \sigma^{i+1}(\beta) \right) \sigma^{k+1}(y) = \alpha - \beta.$$

□

Problem 3.2.1 (UCLA Spring 2015 Problem 6). Let $\mathbb{C}/L/K$ be field extensions such that K contains a p-th root of unity, where p is prime. Show L/K is a degree p Galois extension iff there is an $a \in K$ that is not a p-th root in K, such that $L = K(a^{\frac{1}{p}})$.

Proof. Suppose there exists such an element a. Then, $m_a | x^p - a$, so $x^p - a$ does not split over K. Moreover, since $a^{\frac{1}{p}}$ is a root of $x^p - a$, so is $\zeta_p^k a^{\frac{1}{p}}$ for all $0 \leqslant k \leqslant p-1$. Now, consider the automorphism $\sigma \in \mathrm{Gal}(L/K)$ given by $\sigma(a^{\frac{1}{p}}) = \zeta_p a^{\frac{1}{p}}$. Since the Galois group of L/K sends permutes roots of $x^p - a$, it follows that every element of $\mathrm{Gal}(L/K)$ takes the form σ^k for some $0 \leqslant k \leqslant p-1$. For any such k, since p is prime, one thus has $\langle \sigma^k \rangle = \langle \sigma \rangle \cong \mathbb{Z}_p$, so $\mathrm{Gal}(L/K) \cong \mathbb{Z}_p$. Moreover, since the extension $K(a^{\frac{1}{p}})$ is separable (as it is over a perfect field), and $m_a | x^p - a$, where the latter splits over L, it must be that L is the splitting field of a separable polynomial, so L/K is a Galois extension with Galois group $\mathbb{Z}_p$.

Conversely, suppose L/K is a degree p Galois extension. In particular, it is cyclic, with Galois group $\mathbb{Z}_p$. Then, note that $\beta = \zeta_p^{-1}$ has norm 1. Thus, by Hilbert's Theorem 90, there exists an $\alpha \in L$ such that $\sigma(\alpha) = \zeta_p \alpha$, where $\mathrm{Gal}(L/K) = \langle \sigma \rangle$. In particular, the Galois conjugates of α are $\zeta_p^k \alpha$, so the minimal polynomial of α is $x^p - \alpha^p$, i.e. $a = \alpha^p \in K$ is an element that does not admit a p-th root in K such that $L = K(a^{\frac{1}{p}})$. □

Problem 3.2.2. Let $\mathrm{char}\ F = p > 0$. Show that $x^p - x - a$ either splits over F or is irredicible in F. Conversely, show that if E/F is cyclic of degree p, then E is the splitting field of $x^p - x - a$ for some a.

Proof. Let β be a root of $x^p - x - a$ in some extension of F. If $\beta \notin F$, then $a = \beta^p - \beta$, and the roots of

$$x^p - x - a = x^p - x - (\beta^p - \beta) = (x - \beta)^p - (x - \beta) = 0$$

are $\beta, \beta + 1, ..., \beta + p - 1$, since $y^p - y$ splits over $\mathbb{F}_p$. Thus if $x^p - x - a$ was reducible over F, one of the factors would be a product of the form $(x - (\beta + n_1))...(x - (\beta + n_k))$, and

the second coefficent of this polynomial is $n_k\beta + a, a \in \mathbb{F}_p$, which is in F iff $n_k = 0, p$. Since there are p roots, it thus follows that $x^p - x - a$ is either completely reducible or irreducible over F.

Conversely, suppose E/F is cyclic of degree p. Let $\beta \in E \backslash F$. By Hilbert Theorem 90, $\mathrm{Tr}_{K/k}(1) = 0$, so there exists $\alpha \in E$ such that $1 = \sigma(\alpha) - \alpha$. Then, the conjugates of α are $\alpha + 1, ..., \alpha + p - 1$, so $m_\alpha = x^p - x - a$ for $a = \prod_{k=0}^{p-1}(\alpha + k)$ is an irreducible polynomial with splitting field E. □

Let B be a subgroup of k^* such that $k^{m*} \subset B$ and let $K_B = k(B^{\frac{1}{m}})$. Then K_B is Galois and abelian extension
Lemma2:Let $G = Gal(K_B/k)$.Then we have a bilinear map $\langle , \rangle : G \times B \to \mu_m$ by $\sigma \in G$, $a \in B$ and $\alpha^m = a \to \langle \sigma, a \rangle = \frac{\sigma\alpha}{\alpha}$.The kernel on the left is 1 and the kernel on the right is k^{*m}. The extension K_B/k is finite if and only if $[B : k^{*m}]$ is finite. In that case, $B/k^{*m} \cong \hat{G} = Hom(G, \mu_m)$. Proof : We have K_B Galois as this is a spliting field. We need to check $\langle \sigma, a \rangle = \frac{\sigma\alpha}{\alpha}$ is independent of the m-th root α of a. For the different root of unity, it is $\alpha' = \zeta_n\alpha$ so $\frac{\sigma\alpha'}{\alpha'} = \frac{\zeta\sigma\alpha}{\alpha}$. We can easily check this map is blinear. The kernel on the right, if $\langle \sigma, a \rangle = 1$ for all σ in G,consider the field $k(a^{\frac{1}{m}})$. If $a^{\frac{1}{m}}$ is not in k, then there is an automorphism τ of $k(a^{\frac{1}{m}})$ over k which is not identity and it has an extension to K_B. Call the extension $\overline{\tau}$. $\rangle\overline{\tau}, a\rangle \neq 1$.
That yeild isomorphism $G \cong Hom(B/k^{m*}, \mu_m)$.
Finally see the duality of the finite abelian group $G \times G'$. The commutation of the coproduct gives $Hom(G \times G', S^1) \cong Hom(G, S^1) \times Hom(G', S^1)$. Without loss of generality, we can assume G is cyclic. The $\chi \in Hom(G, S^1)$ is determined by the value of the generator. We have d choice of image. χ is also cyclic. Thus $G \cong B/k^{m*}$.
Proof of the problem Keep in mind of this isomorphism, we have $Gal(\mathbb{Q}(\mu_n)(\sqrt[d_1]{p_1}, \ldots, \sqrt[d_n]{p_n})/\mathbb{Q}(\mu_n)) \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$

Corollary 3.2.1. $\mathbb{Q}(\sqrt[3]{p_1} \ldots \sqrt[3]{p_n} \ldots)/\mathbb{Q}$ *is infinite degree extension.*

Proof. We can see the Galois group of $\mathbb{Q}(\omega, \sqrt[3]{p_1} \ldots \sqrt[3]{p_n} \ldots)/\mathbb{Q}(\omega)$ □

4 Representation Theory

4.1 Languages of Representation Theory

A **representation (rep)** ρ of a group G on a vector space V of dimension n over a field k can be defined in the the following three equivalent ways:

(a) By letting V be a G-space, where every $g \in G$ acts linearly on V, i.e. $g(cv) = cg(v)$ and $g(v_1 + v_2) = g(v_1) + g(v_2)$.

(b) By specifying a group homomorphism $\rho : G \to \mathrm{GL}_n(V) \cong M_n(k)^\times$

(c) By specifying a $k[G]$-module structure on V.

We refer to ρ or V as the representation, and to $\dim V$ as the dimension of the representation. Each of the three languages above is useful when considering certain properties of representations, so we will switch between them freely.

Definition 4.1.1. Two reps

$$\rho_1 : G \to \mathrm{GL}_n(V), \rho_2 : G \to \mathrm{GL}_m(W)$$

are **isomorphic** if they are isomorphic as $k[G]$-modules, i.e. if there exists a vector space isomorphism $\phi : V \to W$ such that $\phi(gv) = g\phi(v)$ for all $g \in G$. Clearly, if $V \cong W$, then $\dim V = \dim W$.

Thus, if $\dim V = \dim W = n$, $V \cong W$ as reps iff there exists a matrix $P \in M_n(k)^\times$ such that $P\rho_1(g)P^{-1} = \rho_2(g)$ for all $g \in G$.

Definition 4.1.2. A homomorphism $\phi : V \to W$ of representations is a homomorphism of V, W as $k[G]$-modules. ϕ is called an **intertwiner**, and the space of intertwiners is denoted as $\mathrm{Hom}_G(V, W)$ or $\mathrm{Hom}_{k[G]}(V, W)$.

Definition 4.1.3. A representation ρ is **irreducible** (irrep) if V is a simple $k[G]$-module, and **indecomposable** if V cannot be written as a nontrivial direct sum of (left) submodules.

Theorem 4.1.1. *$k[G]$ is semisimple iff char k $\nmid |G|$. Moreover, if k is algebraically closed,*

$$k[G] \cong M_{n_1}(k) \times ... \times M_{n_j}(k),$$

where G has precisely j irreps of degrees $n_1, ..., n_j$ respectively.

Lemma 4.1.1 (Schur's Lemma)**.** *If V_i, V_j are irreps over $\mathbb{C}$,*

$$\dim Hom_G(V_i, V_j) = \delta_{ij}.$$

Proof. There are no nonzero homomorphisms between nonisomorphic simple modules, and if $V_i \cong V_j$, since $\mathbb{C}$ is algebraically closed, $\mathrm{End}_G(V_i) = D$ is a division algebra over $\mathbb{C}$, so $\mathrm{End}_G(V_i) = \mathbb{C}$. Thus, $\dim \mathrm{Hom}_G(V_i, V_i) = 1$, given by the scalar matrices. □

Remark 4.1.1. From the theorem, it follows that any rep of a finite group where the field characteristic does not divide order of the group is semisimple, i.e. a direct sum of indecomposable reps. In this case, irreducible representations are equivalent to indecomposable representations. Thus, an irrep is a vector space V with no nontrivial G-invariant subspaces W, i.e. $GW \subset W$.

In general, one is interested in finding all irreps of a given group over (typically) $\mathbb{C}$. In this case, one should use the following facts:

(a) $n_1^2 + ... + n_j^2 = |G|$.

(b) j is the number of conjugacy classes in $|G|$.

(c) $\left|\frac{G}{[G,G]}\right|$ is the number of 1-dimensional irreps of G.

(d) The dimension of every irrep divides $\left|\frac{G}{Z(G)}\right|$.

4.2 Character Theory

Definition 4.2.1. For a finite-dimensional rep ρ, $g \to \mathrm{Tr}(\rho(g))$ defines a map $\chi_\rho : G \to k$ known as the **character** of ρ. It is easy to check that characters are constant on conjugacy classes of G, $\chi_\rho(g)$ is the sum of eigenvalues of $\rho(g)$, and $\chi_\rho(1) = \dim \rho$.

Remark 4.2.1. The word character is also used to refer to the one-dimensional irreps of a group G, i.e. the characters of a group G.

Remark 4.2.2. Since $\rho \cong \rho'$ iff for some $P \in \mathrm{M}_n(k)^\times$, $P\rho(g)P^{-1} = \rho'(g)$, $\rho \cong \rho'$ implies $\chi_\rho = \sum_{i=1}^n \lambda_i = \sum_{i=1}^n \chi_{\rho'}$.

Remark 4.2.3. If $\rho : G \to \mathrm{GL}(V)$ is a finite-dimensional representation of a finite group over $\mathbb{C}$, then if $g^m = 1$, $\rho(g)^m = I$, i.e. if $\{\lambda_i\}$ are the eigenvalues of $\rho(g)$, then $\lambda_i^m = 1$, i.e. λ_i is an m-th root of unity. Particularly, $\lambda_i^{-1} = \overline{\lambda_i}$, so

$$\chi_\rho(g^{-1}) = (\mathrm{Tr} \circ \rho)(g^{-1}) = \sum_i \lambda_i^{-1} = \sum_i \overline{\lambda_i} = \overline{\chi_\rho(g)}.$$

Theorem 4.2.1. *The characters of irreps of a finite group G form an orthonormal basis for the space of* ***class functions*** *(functions $\phi : G \to k$ constant on conjugacy classes) with respect to the inner product*

$$\langle \chi_\rho, \chi_\sigma \rangle = \frac{1}{|G|} \sum_{g \in G} \rho(g)\sigma(g^{-1}).$$

Particularly, for a finite-dimensional representation of a finite group over $\mathbb{C}$, the inner product is equivalently written as

$$\langle \chi_\rho, \chi_\sigma \rangle = \frac{1}{|G|} \sum_{g \in G} \rho(g)\overline{\sigma(g)}.$$

Proof. Over $\mathbb{C}$, orthogonality follows from Schur's lemma. In general, this theorem requires some work. □

Corollary 4.2.1. *If char k $\nmid |G|$, the character uniquely defines a representation ρ, i.e. $\rho \cong \rho'$ as representations iff $\chi_\rho = \chi_{\rho'}$.*

Proof. The forward direction follows from the remark. For the backward direction, suppose $V \cong W$ are isomorphic representations. Decompose $V = \bigoplus_i V_i^{m_i}, W = \bigoplus_i W_i^{n_i}$ into irreps. Then, the characters of V and W are

$$\chi_V = \sum_i m_i \chi_{V_i} = \sum_i n_i \chi_{W_i} = \chi_W,$$

and since characters of irreps are a basis, the sums must be identical. □

Corollary 4.2.2. *V is an irrep iff $\langle \chi_V, \chi_V \rangle = 1$.*

Proof. One direction follows from the theorem. For the other direction, use the previous corollary and the fact that $m_i, n_j \in \mathbb{Z}^+$ to get that $m_i = n_i = 1$ for exactly one choice of i. □

Corollary 4.2.3. *If a rep V contains an irrep V_i exactly n_i times, then $\langle \chi_V, \chi_{V_i} \rangle = n_i$. More generally, if $V = \bigoplus_i V_i^{m_i}, W = \bigoplus_j V_j^{n_j}$, then*

$$\langle \chi_V, \chi_W \rangle = \sum \delta_{ij} m_i n_j.$$

Lemma 4.2.1. *Given representations $\rho_V : G \to V, \rho_W : G \to W$ of G, one can define the following representations:*

(a) The ***direct sum*** *$\rho_{V \oplus W} : G \to GL(V \oplus W)$ given by $\rho_{V \oplus W}(g) = (\rho_V(g), \rho_W(g))$. This corresponds to the direct sum of V and W as $k[G]$-modules, or equivalently, the homomorphism*

$$\rho_{V \oplus W} : g \to \begin{bmatrix} \rho_V(g) & 0 \\ 0 & \rho_W(g) \end{bmatrix}.$$

Clearly, $\chi_{V \otimes W} = \chi_V + \chi_W$, as the eigenvalues of $\rho_{V \oplus W}(g)$ are $\{\lambda_i \cup \mu_j\}$ with eigenvectors $v_i \oplus 0, 0 \oplus w_j$, where $\{\lambda_i\}, \{\mu_j\}$ are the eigenvalues of ρ_V, ρ_W with eigenvectors $\{v_i\}, \{w_j\}$, respectively. A direct sum of reps is obviously never an irrep.

(b) *The* ***tensor product*** $\rho_V \otimes \rho_W : G \times G \to GL(V \otimes W)$ *and an associated tensor product representation* $\rho_{V\otimes W} : G \to GL(V \otimes W)$ *given by* $\rho_{V\otimes W}(g) = \rho_V(g) \otimes \rho_W(g)$. *This corresponds to the tensor product of* V *and* W *as* $k[G]$*-modules, or equivalently, as the Hadamard product*

$$\rho_{V\otimes W} : g \to \rho_V(g) \otimes \rho_W(g).$$

In general, if V, W *are irreps,* $V \otimes W$ *is not an irrep. If* $\{\lambda_i\}, \{\mu_j\}$ *are the eigenvalues of* $\rho_V(g), \rho_W(g)$, *respectively, with eigenvectors* v_i, w_j, $v_i \otimes w_j$ *is an eigenvector with eigenvalue* $\lambda_i\mu_j$. *Consequently* $\chi_{V\otimes W} = \sum_{i,j} \lambda_i\mu_j = \sum_i \lambda_i \sum_j \mu_j = \chi_V\chi_W$.

(c) *The* ***symmetric*** *and* ***alternating*** *representations*

$$Sym^2(V) \cong V \otimes V/\{v \otimes w - w \otimes v\}, \Lambda^2(V) \cong V \otimes V/\{v \otimes w + w \otimes v\}$$

given by

$$\rho_{Sym^2(V)}(g) = \overline{\rho_V(g) \otimes \rho_V(g)}, \rho_{\bigwedge^2(V)}(g) = \overline{\rho_V(g) \otimes \rho_V(g)},$$

with bases $\{v_i \otimes v_j : i \leqslant j\}$ *and* $\{v_i \otimes v_j : i < j\}$ *for a give basis* $\{v_i\}$ *of* V. *Thus,* $\dim Sym^2(V) = \frac{n^2+n}{2}$ *and* $\dim \bigwedge^2(V) = \frac{n^2-n}{2}$. *By the same arguments as above, if* $\{\lambda_i\}$ *are eigenvalues of* $\rho(g)$ *with eigenvectors* $\{v_i\}$, *then* $\{\lambda_i\lambda_j : i \leqslant j\}$ *and* $\{\lambda_i\lambda_j : i < j\}$ *are eigenvalues of* $\rho_{Sym^2(V)}(g), \rho_{\bigwedge^2(V)}(g)$, *respectively, yielding the formulas*

$$\chi_{Sym^2(V)}(g) = \frac{\chi_V(g)^2 + \chi_V(g^2)}{2}, \chi_{\bigwedge^2(V)}(g) = \frac{\chi_V(g)^2 - \chi_V(g^2)}{2},$$

in particular showing that

$$V \otimes V \cong Sym^2(V) \oplus \Lambda^2(V)$$

(which follows from character theory).

(d) *The* ***dual representation*** $\rho_{V^*} : G \to GL(V^*)$ *given by* $\rho_{V^*}(g)(\phi)(-) = \phi(\rho(g^{-1})(-))$. *In particular,* V^* *becomes a* $k[G]$*-module, and the identity above implies*

$$\rho_{V^*}(g) = \rho_V(g^{-1})^T \quad \textit{(which over } \mathbb{C} \textit{ is just the Hermitian adjoint of } \rho_V(g)),$$

motivated by the identity

$$\langle \rho_{V^*}(g)(v), \rho_V(g)(w) \rangle = \langle v, w \rangle.$$

Over $\mathbb{C}$, *if* $\{\lambda_i\}$ *are the eigenvalues of* $\rho_V(g)$, *the eigenvalues of* $\rho_{V^*}(g)$ *are* $\{\overline{\lambda_i}\}$, *so* $\chi_{V^*} = \overline{\chi_V}$. *Thus,* V *is an irrep iff* V^* *is an irrep.*

(e) *The* ***intertwiner representation*** $\rho : G \to GL(Hom_G(V, W))$ *given by* $\rho(g)(\phi(-)) = \rho_2(g)(\phi(\rho_1^{-1}(g)(-)))$. *In particular,* $Hom_G(V, W)$ *is a* $k[G]$*-module. When* V, W *are finite-dimensional, note that there is an isomorphism of* $k[G]$*-modules*

$$V^* \otimes W \cong Hom_G(V, W)$$

$$v^* \otimes w \to \phi(v) = v^*(v)w.$$

Over $\mathbb{C}$, *of the eigenvalues of* $\rho_V(g), \rho_W(g)$ *are* $\{\lambda_i\}, \{\mu_j\}$, *the eigenvalues of* $\rho(g)$ *are* $\{\overline{\lambda_i}\mu_j\}$, *so* $\chi_\rho = \overline{\chi_V}\chi_W$.
Over $\mathbb{C}$, *if* V_i, V_j *are irreps, Schur's lemma yields*

$$\dim Hom_G(V_i, V_j) = \langle \chi_i, \chi_j \rangle,$$

so by linearity one has

$$\dim Hom_G(V, W) = \langle \chi_V, \chi_W \rangle.$$

(f) *Given a finite group G, the* ***(left) regular representation*** $\rho_G : G \to GL_{|G|}(V)$ *is given by the composition of homomorphisms $G \to S_{|G|} \to GL_{|G|}(V)$, where the first homomorphism is induced by the group action of left multiplication, and the second homomorphism is the* ***monomial/permutation representation*** *of S_n, where $\rho(\sigma)(v_i) = v_{\sigma(i)}$ for an ordered basis $\{v_i\}$ of V. In this case,*

$$V \cong k[G] \cong \bigoplus V_i^{n_i},$$

where V_i is an irrep of dimension n_i, as left $k[G]$-modules. This is equivalent to the homomorphism

$$\rho_G : g \to (a_{ij}),$$

where $a_{ij} = \begin{cases} 1 & \text{if } gg_i = g_j \\ 0 & \text{otherwise} \end{cases}$, *where $\{g_i\}$ is a chosen ordered basis of $k[G]$. It immediately follows that* $\chi(g) = \begin{cases} |G| & \text{if } g = 1. \\ 0 & \text{otherwise.} \end{cases}$ *Except for the case $|G| = 1$, the regular representation is not irreducible.*

(g) *For $H \leqslant G$, the* ***restricted representation*** *of a representation $\rho_G : G \to GL(V)$ is the representation $\rho_H : H \to GL(V)$ given by the composition of homomorphisms $H \to G \to GL(V)$. In general, the restriction of an irreducible representation may not be irreducible.*

(h) *Let G be a finite group and $H \leqslant G$ a subgroup, and V be a representation of H. Let $g_1H, ..., g_nH$ be the left cosets of H in G. We now consider the G-space*

$$W = \bigoplus_{i=1}^{n} g_iV$$

where the above is a formal direct sum with $g_iV = \{g_iv : v \in V\}$. with the G-action given by

$$g \cdot \sum_{i=1}^{n} g_iv_i = \sum_{i=1}^{n} g_{j_i}\rho(h_i)v_i,$$

where $gg_i = g_{j_i}h_i \in g_jH$. This is the ***induced representation*** *$Ind_H^G(V)$ of dimension $[G : H]$. As a $k[G]$-module, it is isomorphic to $k[G] \otimes_{k[H]} V$. For example, if $H = \{e\}$ and V is the trivial representation, the induced representation is $k[G] \otimes_{k[H]} k \cong k[G]$ is the regular representation, actin on cosets by $g \cdot (g_iv) = (gg_i)v$. An induced representation of a one-dimensional rep is called a* ***monomial representation****, as it is represented by monomial matrices. By the tensor-hom adjunction,*

$$Hom_{k[G]}(k[G] \otimes_{k[H]} V, W) \cong Hom_{k[H]}(V, Hom_{k[G]}(k[G], W)) \cong Hom_{k[H]}(V, W),$$

leading to the ***Frobenius reciprocity theorem****, which states that for reps V, W of G,*

$$\langle \chi_{Ind_H^G(V)}, \chi_W \rangle = \langle \chi_V, \chi_{Res_H^G(W)} \rangle.$$

The orthogonality relations can be usefully presented in a square **character table**, listing the conjugacy classes and the distinct values of the characters on those classes. In particular, the rows of the character table are orthogonal. By the theory of orthonormal matrices, this yields the orthogonality of columns. The dot product of the conjugacy class sizes with the square of a row yields the order of the group, while the dot product of a column is the ratio $\frac{|G|}{|C_i|}$, where C_i is the corresponding conjugacy class.

4.3 Representation Theory of Specific Groups

Here are some examples of common character tables.

(a) $\mathbb{Z}_n = \langle r \rangle$ has n one-dimensional representations $\rho(r) = \zeta_n^k, 0 \leqslant k \leqslant n-1$ where ζ_n is the n-th root of unity. Moreover,

$$\mathbb{C}[\mathbb{Z}_n] \cong \mathbb{C}^n$$

as $\mathbb{C}[\mathbb{Z}_n]$-modules.

(b) **Representation Theory of** S_n. Aside from the trivial and **alternating** representations of S_n, one may note that the permutation representation V decomposes as the direct sum of a trivial representation given by the subspace

$$W = \{(v_1, ..., v_n) \in V : v_1 = ... = v_n\}$$

and its complement, known as the **standard representation** of S_n. One may directly verify that both representations are irreducible, with $\chi_{W^\perp} = \chi_V - 1$, where $\chi_V(g)$ is the number of indices fixed by $g \in S_n$. Thus, for instance, S_4 has five conjugacy classes and thus five characters - the trivial, alternating, standard, product of standard and alternating, and the remaining two-dimensional one, which can be determined from the orthogonality relations. All can be checked to be irreducible.

Cycle Type	(1)	(2)	(2, 2)	(3)	(4)
Trivial	1	1	1	1	1
Alternating	1	-1	1	1	-1
2-dim.	2	0	2	-1	0
Standard	3	1	-1	0	-1
Standard $\otimes$ Alternating	3	-1	-1	0	1

Table 1: Character Table for S_4.

A similar approach may be taken for S_5, which has 7 irreps. We compute the character of Standard $\otimes$ Standard to be $(16, 4, 0, 1, 1, 0, 1)$, which we know contains the symmetric and alternating characters $(10, 4, 2, 1, 1, 0, 1), (6, 0, -2, 0, 0, 0, 0)$. One directly checks that the alternating square is irreducible. Then, the sum of square of the remaining representations is 50. Since $[S_5, S_5] = A_5$, there are exactly two one-dimensional representations, so the remaining representations both have degree 5. Moreover, one can check that the symmetric square contains of a copy of the trivial representation and a copy of the standard one, yielding an irreducible representation of degree 5.

(c) **Representations of** D_{2n}. From the group presentation

$$D_{2n} = \langle r, s | r^n = s^2 = 1, srs = r^{-1} \rangle,$$

one determines that there are two cases to consider:
n even. When n is even, the conjugacy classes are

$$\{e\}, \{r, r^{n-1}\}, ..., \{r^{\frac{n}{2}}\}, \{s, sr^2, ..., sr^{n-2}\}, \{sr, ..., sr^{n-1}\},$$

giving a total of $\frac{n}{2} + 3$ irreps. Of these, 4 are one-dimensional, given by mapping

$$s \to \pm 1, r \to \pm 1.$$

Conjugacy Class Size	1	10	15	20	20	30	24
Cycle Type	(1)	(2)	(2, 2)	(2, 3)	(3)	(4)	(5)
Trivial	1	1	1	1	1	1	1
Alternating	1	-1	1	-1	1	-1	1
Standard $\otimes$ Alternating	4	-2	0	1	1	0	-1
Standard	4	2	0	-1	1	0	-1
5-Dim in Symmetric Square	5	1	1	1	-1	-1	0
5-Dim in Symmetric Square $\otimes$ Alternating	5	-1	1	-1	-1	1	0
Alternating Square	6	0	-2	0	0	0	1
Symmetric Square	10	4	2	1	1	0	0

Table 2: Character Table for S_5.

n odd. When n is odd, the conjugacy classes are

$$\{e\}, \{r, r^{n-1}\}, ..., \{r^{\frac{n-1}{2}}, r^{\frac{n+1}{2}}\}, \{s, sr^2, ..., sr^{n-1}\},$$

giving a total of $\frac{n-1}{2} + 2$ irreps. Of these, 2 are one-dimensional, given by mapping $s \to \pm 1$. Finally, motivated by the use planar symmetry of D_{2n}, we consider the two-dimensional representations $r \to R_{\frac{2\pi k}{n}}, s \to \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, where R_θ is the rotation matrix by θ degrees. Note that this yields $\frac{n-1}{2}$ distinct representations when n is odd and $\frac{n}{2} - 1$ distinct representations when n is even. Moreover, these are easily checked to be irreducible. Note that we thus account for $\frac{n}{2} - 1 + 4 = \frac{n}{2} + 3$ irreps when n is even and $\frac{n-1}{2} + 2$ irreps when n is odd. Thus, we have completely classified all the representations of D_{2n}, namely,

$$\begin{cases} n \text{ even} & \implies \quad \frac{n-1}{2} - 1 \text{ two-dimensional, 4 one-dimensional representations} \\ n \text{ odd} & \implies \quad \frac{n}{2} - 1 \text{ two-dimensional, 2 one-dimensional representations.} \end{cases}$$

and the corresponding characters may be computed directly,

4.4 Clifford Theory and Induced Representations

Problem 4.4.1 (Spring 2014: Problem 4). Let G be a group and H a normal subgroup of G. Let k be a field and let V be an irreducible representation of G over k. Show that the restriction of V to H is semi-simple.

Proof. This is called Cliford theorem.
Let W be any simple $K[N]$-submodule of V_N. For every $g \in G, gW := \{gw | w \in W\}$ is also a $k[N]$-submodule of V_N, because $N \lhd$ for any $n \in N$, we have $n \cdot gW = g(g^{-1}ng)W = gW$.
Moroever, gW is also simple, since if X were a non-trivial proper $K[H]$-submodule of gW then $g^{-1}X$ would also be a a non-trivial proper submodule of W. Now $\sum gW$ is non-zero and it is a $k[H]$-submodule of V, which is simple, hence $\sum gW = V$. Restricting to H, we obtain that $V_H = \sum gW$ is a sum of simple submodules. Hence semisimple.

□

Problem 4.4.2 (Fall 2022: Problem 6). Let G be a finite group, let V be a finite-dimensional complex vector space and let $\pi : G \to GL(V)$ an irreducible representation. Let H be an abelian subgroup of G. Show that $dim(V) \leqslant [G : H]$.

Proof. This proof is from Serre's book on representation theory.
Let $\rho : G \to GL(V)$ be an irreducible representation of G. Through the restriction to A, we have a representation $\rho|_H : H \to GL(V)$ of H. Let $W \subset V$ be an irreducible subrepresentation of ρ_H. As H is abelian, $\dim(W) = 1$.
Let V' be the vector subspace of V generated by the images of $\rho_s W$, where s ranges over G. Note that as ρ is irreducible, V' is stable under G, thus $V' = V$. But for $s \in G$ and $h \in H$, we have

$$\rho_{sh} W = \rho_s \rho_h W = \rho_s W$$

as W is an irreducible subrepresentation of A, and thus stable under A. Thus the number of distinct $\rho_s W$ is at most equal to $[G : H]$. Since V equals the sum of $\rho_s W$, we have the desired inequality. □

5 Commutative Ring Theory

5.1 Noetherian Rings, PID, and UFD

Idea: Whenever you have a nilpotent ideal (an ideal I such that $I^n = 0$ for some $n \in \mathbb{N}$), you can decompose it using a filtration.

$$\begin{aligned} I &\supset I^2 \supset I^3 \supset \cdots \supset I^n = 0 \\ I &\cong \frac{I}{I^2} \oplus I^2 \\ &\cong \frac{I}{I^2} \oplus \frac{I^2}{I^3} \oplus \cdots \oplus \frac{I^{n-1}}{I^n} \oplus I^n \\ &\cong \frac{I}{I^2} \oplus \cdots \oplus \frac{I^{n-1}}{I^n} \end{aligned}$$

5.2 Fraction ring/ Localization

5.3 Dedekind Ring

Definition 5.3.1 (Divisibility of ideal)**.** Let $\mathfrak{a}, \mathfrak{b} \subset R$ be ideals with $\mathfrak{b} \neq 0$ We say $\mathfrak{a}$ is divisible by $\mathfrak{b}$ if there is an ideal $\mathfrak{c} \subset R$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$

Definition 5.3.2 (Dedekind domain)**.** The integral domain R is a Dedekind if for any two ideals $\mathfrak{a} \subset \mathfrak{b} \neq 0$, we have $\mathfrak{b}$ divides $\mathfrak{a}$.

Basic properties of Dedekind rings:

Lemma 5.3.1. *Every ideal of a Dedekind ring is finitely generated projective R-module.*

Proof. Let $\mathfrak{a} \subset R$ be an ideal. if $\mathfrak{a} = 0$ then there is nothing to show. When $\mathfrak{a}$ is nontrivial ideal, then $a \in \mathfrak{a}$ $aR = \mathfrak{a}\mathfrak{b}$ for some ideal $\mathfrak{b} \subset R$. Write $a = \sum x_i y_i$ for $x_i \in \mathfrak{a}, y_i \in \mathfrak{b}$. Define $f : R^n \to \mathfrak{a}$ by $f(r_1 \dots r_n) = \sum r_i x_i$. That is surjective, so there is a exact sequence

$$0 \longrightarrow \ker f \longrightarrow R^n \xrightarrow{f} \mathfrak{a} \longrightarrow 0$$

this last morphism is split by $g : \mathfrak{a} \to R^n$ by $g(z) = (\frac{zy_i}{a})_i \in R^n$. Thus $\mathfrak{a}$ is the direct summand of R^n. □

Definition 5.3.3 (Fractional Ideal)**.** Let R be a Dedekind domain and F be its quotient field. A fractional ideal is finitely generated R-submodule of F

Well known properties of the Dedekind ring is that any prime ideal can be uniquely factorized into the products of prime ideals. In the case of the principal ideal we have the clear understanding of the fraction ideal namely pick $a \in R$,

$$aR = \mathfrak{p}_1^{\ell_1} \dots \mathfrak{p}_n^{\ell_n} \implies \frac{1}{a}R = \mathfrak{p}_1^{-\ell_1} \dots \mathfrak{p}_m^{-\ell_m}$$

How about the general ideal it is unclear how to define the inverse fractional ideal, unlike principal cases, next problem suggest a way to make it inverse.

Problem 5.3.1 (Stanford Qualifying exam). Let R be the Dedekind ring, I be the ideal of the Dedekind ring and $F := Frac(R)$. Define

$$I' := \{y \in K \mid yI \subset R\}$$

show I' are finitely generated as R-module and $I \otimes I' \cong R$ defined by $i \otimes j \to ij$.

Proof. We want to see that I' is the inverse fractional ideal of I. Pick any elements of $a \in I$ then by the divisibility property of the ideal we can find the J such that $IJ = aR$. Since fractional inverse of a is defined, we define $J' = \frac{1}{a}J$. Here we prove $J' = I'$. First of all $J' \subset F$ and pick any elements $j \in J$, $jI \subset R$. That implies $J' \subseteq I'$. On the other hand, $II' \subset R = IJ'$ so $I' \subset J'$. Thus $I' = J'$. In particular J is finitely generated, so J' is also fintely generated. The surjection for $I \otimes \frac{1}{a}J \to aR$ is clear. On the other hand since J is a projective module, in particular flat. There exist a exact sequence

$$0 \to I \to R$$

$$0 \to I \otimes J' \to R \otimes J$$

But flatness preserve injection, so we show what we want. □

Idea: Fractional ideals in Dedekind rings are ideals divided by non-zero elements a.

Problem 5.3.2 (UCLA 2013 Fall Problem 6). Let I be an ideal of a commutative ring and $a \in R$. Suppose the ideals $I + Ra$ and $(I : a) := \{x \in R : ax \in I\}$ are finitely generated. Prove that I is also finitely generated.

Proof. We have $(I + Ra)/Ra \cong I/(I \cap Ra) = I/a(I : a)$. Therefore if $I + Ra$ is finitely generated, its quotient is also finitely generated. We have an exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^n & \longrightarrow & R^{n+m} & \longrightarrow & R^n & \longrightarrow & 0 \\ & & \downarrow & & \vdots & & \downarrow & & \\ 0 & \longrightarrow & a(I:a) & \longrightarrow & I & \longrightarrow & I/a(I:a) & \longrightarrow & 0 \end{array}$$

then by the 4-lemma for the epismorphism the middle arrow is also episomorphism □

5.4 Localization

Recall that for a commutative ring A and a multiplicatively closed subset $1 \in S \subset A$, we can define the localization with $S^{-1}A$ as the set of equvalence classes $\overline{\frac{r}{s}}$, where $\overline{\frac{r_1}{s_1}} = \overline{\frac{r_2}{s_2}}$ if for some $s \in S$, $s(r_1 s_2 - r_2 s_1) = 0$. In particular, one typically considers the following types of localization:

(a) When R is an integral domain, the field of fractions of $F(R)$ of R is formally defined as the localization $S^{-1}R$ at $S = R\backslash\{0\}$.

(b) For a prime ideal $\mathfrak{p} \subset R$, one can consider localization at the prime ideal $R_\mathfrak{p} = S^{-1}R$ for $S = R\backslash\mathfrak{p}$. It is necessary that $\mathfrak{p}$ be prime for S to be multiplicately closed, as $a, b \notin \mathfrak{p}$ implies $ab \notin \mathfrak{p}$. Localization at a prime ideal yields a local ring with maximal ideal $\mathfrak{p}R_\mathfrak{p}$.

(c) For $r \in R$ not nilpotent and $S = \{1, r, r^2, ...\}$, one can construct the localization $S^{-1}R = R_r \cong R[\frac{1}{r}]$.

There is a natural map $R \to S^{-1}R$, which is injective if R is an integral domain. For an R-module M, one can the localization functor $S^{-1} : \text{R-Mod} \to S^{-1}R\text{-Mod}$ sending M to $S^{-1}R \otimes_R M \cong S^{-1}M$. The localization functor is exact, i.e. $S^{-1}R$ is a flat R-module. In particular, $\overline{m} = 0$ in $S^{-1}M$ iff $sm = 0$ for some $s \in S$.
Additionally, one has the following ideal correspondence theorem: there is a bijection between prime (maximal) ideals of $S^{-1}R$ and prime (maximal) ideals of R not intersecting S.

Finally, localization commutes with many familiar operations, including quotients, direct sums, tensor products, etc.

Problem 5.4.1. Let R be an integral domain, M be an R-module. Show M is R-torsion-free iff $M_\mathfrak{m}$ is $R_\mathfrak{m}$-torsion free for every maximal ideal $\mathfrak{m} \subset R$.

Proof. Suppose M is not torsion free. Then, for some $r, m \neq 0$, $rm = 0$. Let $\mathfrak{m} \supset \text{Ann}_R(m)$ be a maximal ideal. Then, in $M_\mathfrak{m}$, $\overline{rm} = 0$. But $\overline{r} \neq 0$ since R is an integral domain, and $\overline{m} \neq 0$ since $\text{Ann}_R(m) \cap S = \varnothing$.
Conversely, suppose $M_\mathfrak{m}$ is not torsion-free for some $\mathfrak{m}$. Then, $\overline{\frac{r}{s}m} = \overline{0}$ for $r, s, m \neq 0$. so for some $s' \in S$, $s'rm = 0$. But since R is an integral domain, this implies $s'r \neq 0$ annihilates m, so M is not torsion-free. □

Problem 5.4.2. Let R be a Noetherian commutative ring. Show that if $\text{Nil}(R) = 0$ and the localization $R_\mathfrak{m}$ of R at every maximal ideal is a finite ring, then R is finite.

Proof. Note that $R_\mathfrak{m}$ being finite is a very strong condition, as it implies that $R_\mathfrak{m}$ is Artinian. By the Hopkins-Levitzki theorem, this implies that $R_\mathfrak{m}$ has dimension 0, which by the correspondence theorem for localization implies that R has dimension 0. Then, by Hopkins-Levitzki again, since R is Noetherian and dimension 0, R is Artinian. We claim that R has finitely many maximal ideals. First, note that for a collection of maximal ideals, $\prod \mathfrak{m}_i = \bigcap \mathfrak{m}_i$. Indeed, if there were infinitely many maximal ideals, by DCC we would have that $\mathfrak{m}_{k+1} \supset \bigcap_{i=1}^k \mathfrak{m}_i = \prod_{i=1}^k \mathfrak{m}_k$, which implies that $\mathfrak{m}_j \subset \mathfrak{m}_{k+1}$ (since maximal ideals are prime), which is a contradiction.
In particular, R has finitely many prime ideals, all of which are maximal, so by the Chinese

Remainder Theorem,

$$R \cong R/\mathrm{Nil}(R) \cong R/(\mathfrak{m}_1 ... \mathfrak{m}_k) \cong R/\mathfrak{m}_1 \times ... \times R/\mathfrak{m}_k.$$

Now, localizing a field does not change the field, so $\mathfrak{m}_i$ yields $|R/\mathfrak{m}_i| = |(R/\mathfrak{m}_i)_{\mathfrak{m}_i}| < \infty$, so R is finite. □

Problem 5.4.3. Let A be a comm. ring, $S = \{1, s, s^2, ...\}$. Show that the following are equivalent:

(a) The canonical morphism $A \to S^{-1}A$ is surjective.

(b) For $N > 0$ large, $s^n A = s^N A$ for all $n \geqslant N$.

(c) For n large, $s^n A$ is generated by an idempotent.

Proof. (1) $\implies$ (2): Note that it suffices to show that $s^N = rs^{N+1}$ for some $r \in R$, as then $s^N = r^{n-N}s^n$. Suppose the canonical morphism is surjective. Then, for $\overline{\frac{1}{s}}$, there is an $r' \in R$ such that $\overline{r'} = \overline{\frac{1}{s}}$, i.e. for some

$$s^k(r's - 1) = r's^{k+1} - s^k = 0$$

for some $k > 0$ i.e. $s^k = r's^{k+1}$. But this precisely proves the claim for $r = r'$ and $N = k$.
(2) $\implies$ (3): Suppose $s^n A = s^N A$ for all $n \geqslant N$ for some N. Then, in particular, $s^N = s^{N+1}r = s^N(sr)$ for some $r \in R$. Let $e = s^N r^N$. Then, e is an idempotent, since

$$(s^N r^N)(s^N r^N) = (rs)^N (s^N) r^N = s^N r^N,$$

and $s^N r^N A = s^N A$, as $s^N(s^N r^N) = (rs)^N s^N = s^N$. Thus, for $n \geqslant N$, $s^n A = s^N A = eA$ is generated by an idempotent e.
(3) $\implies$ (2): Suppose that for n large enough, $s^n A$ is generated by an idempotent e. It suffices to show that for some $r \in R$, $\overline{r} = \overline{\frac{1}{s}}$, as then an $r^k r'$ will map to any arbitrary element $\overline{\frac{r'}{s^k}}$, making the canonical morphism surjective. But this holds iff for some $k > 0$, $s^k(rs - 1) = 0$, i.e. $s^{k+1}r = s^k$, i.e. $(rs)s^k = s^k$. Let $s^N A = s^{N+1}A = eA$, so $s^N = s^{N+1}r = (rs)s^N$. Then, for $k = N$ and that choice of r, the claim follows.

□

6 Noncommutative Ring Theory

6.1 Jacobson Radical and Nilradical

For any left R-module M, the Jacobson radical, $J(M)$ is defined to be the intersection of all maximal left (or equivalently, right) submodules.

Jacobson radical is useful because it can measure if a module is semi-simple or not due to the the following propositions.

Theorem 6.1.1. *Let M be a left R module. Then if M is semi-simple then $J(M) = 0$. If M is artinian then and $J(M) = 0$ then M is semi-simple.*

Proof. When M is semi-simple module, M can be written as the direct sum of simple module $M = M_1 \oplus M_2 \oplus \dots M_n$. Their only intersection is $\{0\}$ so the first statement is true.
Second statement I am not sure I want to type it. □

for the *ring* there are alternative characterizations for the Jacobson radical Jaconson radical is a set is $x \in J(R) \subset R$ such that $1 - xy \in R^\times$ for any $y \in R$.

The Jacobson radical is also a two-sided ideal for the ring.

Nilradical $Nil(R)$ of the ring R is set of all nilpotent elements of the ring.

Proposition 6.1.1. *When R is commutative ring, $Nil(R)$ is the intersection of the all prime ideals.*

Proof. $\implies$ Take a nilpotent elements a such that $a^n = 0$. All prime ideal $\mathfrak{p}_i$ contains 0. In particular for a prime ideal there exist i such that $a^i \in \mathfrak{p}_i$. So $\cap \mathfrak{p}_i$ contains all the nilpotent elements.

$\impliedby$ We can show this statement by the localization and Zorn's lemma.
The first methods. Suppose $\cap \mathfrak{p}_i$ contains elements a that is not a nilpotent. There is a set of ideal $P = \{I | \exists k \in \mathbb{Z} : a^k \notin I\}$. By the Zorn's lemma there exist a maximal I' among the set of P. We will prove this I' is indeed a prime ideal so that b should not be contained in $\cap \mathfrak{p}_i$. Assume this is not a prime ideal then there exist an elements $f, g \notin I'$ but $fg \in I$. But then by the maximality of the I' $I' + (f)$ and $I' + (g)$ contains some power of a but $a^r a^s \in I' = I' + (fg)$ is the contradiction. □

Idea: If you want to prove an element has redundant things contained in a maximal or prime ideal, we can use the Zorn's lemma to construct a prime ideal or maximal ideal that does not contain an element.

We can apply the similar idea for the next problem.

Problem 6.1.1 (UCLA 2018 Fall Problem 5). Let R be a commutative ring. Show the following:

(a) Let S be a non-empty saturated multiplicative set in R, i.e. if $a, b \in R$, then $ab \in S$ if and only if $a, b \in S$. Show that $R \backslash S$ is a union of prime ideals.

(b) If R is a domain, show that R is a UFD if and only if every nonzero prime ideal in R contains a non-zero principal prime ideal.

Definition 6.1.1. Let I be a left ideal of a ring. We say I is nil if for every $a \in I$, there exists some positive integer n such that $a^n = 0$. We say that I is nilpotent if $I^n = (0)$ for some positive integer n. Clearly if I is nilpotent, then I is also nil.

Proposition 6.1.2. *The Jacobson radical of a ring contains every nil left ideal of the ring.*

Proof. Let I be a nil left ideal of a ring R. Let $x \in I,\ r \in R$. Then $rx \in I$ and so rx is nilpotent. Hence $(rx)^n = 0$ for some positive integer n and so $1 + rx + \dots + (rx)^{n-1}$ is the inverse of $1 - rx$. Thus $1 - rx$ is invertible for all $r \in R$ and so $x \in J(R)$. □

6.2 Module Homomorphisms

Let R be a noncommutative ring, and suppose M, N are left R-modules. We will denote this situation as ${}_R M, {}_R N$. Then, in general,

$$\mathrm{Hom}_{\text{R-Mod}}({}_R M, {}_R N)$$

has *no module structure,* since if we attempted to define a left R-module structure by $(r \cdot \phi)(m) = \phi(rm)$, $r \cdot \phi$ would not be a left R-module homomorphism, since

$$sr\phi(m) = s(r \cdot \phi)(m) \neq (r \cdot \phi)(sm) = \phi(rsm) = rs\phi(m).$$

However this may be remedied by imposing additional structure on M, N. For instance, $\text{Hom}_{\text{R-Mod}}({}_RM_R, {}_R N)$ is a left R-module by $(r \cdot \phi)(m) = \phi(mr)$. Likewise,

$$\text{Hom}_{\text{R-Mod}}({}_RM, {}_R N_R) \in \text{Mod-R},$$

$$\text{Hom}_{\text{Mod-R}}({}_RM_R, N_R) \in \text{Mod-R},$$

$$\text{Hom}_{\text{Mod-R}}(M_R, {}_R N_R) \in \text{R-Mod},$$

and we can similarly establish (R, R)-bimodule structures. Thus, for instance, it does indeed hold that

$${}_RM \cong \text{Hom}_{\text{R-Mod}}({}_RR_R, {}_R M)$$

for an arbitrary left R-module M. Finally, there is also a ring structure given by

$$\text{Hom}_{\text{R-Mod}}(R, R) \cong R^{op}, \phi \to \phi(1),$$

where each element on the left $\phi : r \to r\phi(1)$ is identified with right multiplication by $\phi(1)$. The opposite ring structure follows from composition of maps on the left and multiplcation on the right, given by

$$\psi \circ \phi \to \phi(1)\psi(1).$$

In particular, this yields a quick solution of the module problem on the qualifying exam:

Problem 6.2.1 (UCLA 2018 Fall Problem 5). Let R be a ring. Show that if $R^n \cong R^m$ as left R-modules, $R^n \cong R^m$ as right R-modules.

Proof. Note that $\text{Hom}_{\text{R-Mod}}(-, R)$ is a functor (would probably need to prove in exam), and therefore it preserves isomorphisms. Thus,

$${}_RR^n \cong_R R^m \implies \text{Hom}_{\text{R-Mod}}({}_RR^n, {}_R R_R) \cong \text{Hom}_{\text{R-Mod}}({}_RR^m, {}_R R_R) \in \text{Mod-R},$$

where the latter immediately implies

$$R_R^n \cong R_R^m$$

by commutativity of Hom with direct sums and the isomorphism of right R-modules

$$\text{Hom}_{\text{R-Mod}}({}_RR, {}_R R_R) \cong R_R, \phi \to \phi(1),$$

(since $\phi \cdot r \to \phi(r) = \phi(1) \cdot r$) (alternatively, one can see that $\text{Hom}_{\text{R-Mod}}(R, R) \cong R^{op} \cong R$ as both left and right R-modules). □

6.3 Artinian and Semi-simple Rings

6.4 Morita Equivalence

This section outlines the proof of Morita equivalence.

Definition 6.4.1. Let R, S be rings. We say R is **Morita equivalent** to S (writing $R \sim S$), if there exists an equivalence of categories R-Mod $\cong$ S-Mod.

The goal is to understand the necessary and sufficient conditions for two rings to be Morita equivalent. The following result from homological algebra proves extremely useful:

Theorem 6.4.1. *(Eilenberg-Watts) Let F : R-Mod $\to$ S-Mod be a cocontinuous functor (i.e. one that commutes with all small colimits). Then $F(-) \cong_S P_R \otimes_R -$ for an (S, R)-bimodule P.*

Thus, every right exact functor between categories of modules is naturally isomorphic to a tensor product. In particular, if R-Mod and S-Mod are equivalent, there exist a (S, R)-bimodule M and a (R, S)-bimodule N such that ${}_SM_R \otimes_R N_S \cong S$ and ${}_RN_S \otimes_S M_R \cong R$ as bimodules. Moreover, by the tensor-hom adjunction,

$$\mathrm{Hom}_R(-, N \otimes_S L) \cong \mathrm{Hom}_S(M \otimes_R -, M \otimes_R N \otimes_S L) \cong \mathrm{Hom}_S(M \otimes_R -, L) \cong \mathrm{Hom}_R(-, \mathrm{Hom}_S(M, L)),$$

so $N \otimes_S - \cong \mathrm{Hom}_S(M, -)$ are naturally isomorphic as functors. Moreover,

$$S \cong \mathrm{Hom}_S(S_S, S_S) \cong \mathrm{Hom}_R(S_S \otimes_S M, S_S \otimes M) \cong \mathrm{End}_R(M_R).$$

Finally, since M, N are images of R, S, respectively under an equivalence, they are both finitely generated projective modules. Now, we attempt to reverse this process, starting with two projective modules and using them to form an equivalence of categories.

Definition 6.4.2. A collection of **generators** in a category $\mathcal{C}$ is a family of objects $\mathfrak{G}$ such that for any two distinct morphisms $f, g : Y \rightrightarrows Z$, there exists an object $X \in \mathfrak{G}$ and a morphism $h : X \to Y$ such that $gh \neq fh$. If the family contains one element, that element is called a **generator**.

Example 6.4.1. In R-Mod, any free module R^n is a generator, as for any two distinct maps $f, g : Y \rightrightarrows Z$, and $y \in Y$ such that $f(y) \neq g(y)$, $h : R^n \to Y$ given by $h(e_1) = y, h(e_i) = 0$ for $i \geqslant 2$, satisfies $gh \neq fh$.

Remark 6.4.1. A module M in R-Mod is a generator iff R is a direct summand of M^k for some $k \in \mathbb{N}$.

Definition 6.4.3. A projective finitely generated (left) R-module that is a generator is called a **progenerator.**

Remark 6.4.2. From the two claims above and the definition of a projective module, it follows that M is a progenerator if $M^a \cong R^b$ for some $a, b \in \mathbb{N}$.

Remark 6.4.3. If $R \sim S$ and M, N are given as above, ${}_SM, {}_RN$ are progenerators.

We are now able to give the full statement of Morita equivalence.

Theorem 6.4.2. *(Morita Equivalence) $R \sim S$ iff $S \cong End_R(P_R) \cong eM_n(R)e$ for some progenerator P_R in R-Mod and a full idempotent $e \in M_n(R)$. Moreover, if F, G form an equivalence of categories, then the equivalence is given by $F(-) \cong P_R \otimes -, G(-) \cong Hom_S({}_SP, -)$.*

If one chooses $P_R = R^n$, then $R \sim \mathrm{End}_R(R^n_R) \cong M_n(R)$, so R and $S = M_n(R)$ are Morita equivalent under ${}_RM \to R^n \otimes_R M$ and ${}_SN \to \mathrm{Hom}_S({}_SR^n, {}_SN)$. Since Morita equivalence is categorical, all categorical properties of modules are preserved under the equivalence. Namely, the following properties (all of which can be defined in terms of universal properties) of modules are preserved:

(a) Simple/semisimple

(b) Injective/projective/flat

(c) Faithful

(d) Finitely generated/presented

(e) Artinian/Noetherian

Moreover, the following properties are preserved across the rings R and S (which can be also described categorically):

(a) Simple/semisimple

(b) Artinian/Noetherian

(c) Centers, i.e. $Z(R) \cong Z(S)$.

Under the categorical equivalnces simplness of the module M can be phrased categorically for any nonzero morphism from M is a injective. Under the categorical equivalence, injectiveness is preserved, thus simpliness preserved. Semisimplness is a direct sum of the simple module. Injective, projective can be written in the language of the epi/mono by the definition so it is already categorical. Noetherian/Artinian property is preserved becauae inclusion is preserved and there are only finitely many inclusion. Ideal is not a subring, however we can reformulate the existence of the chain of the ideal

$$I_1 \subset I_2 \subset \dots I_n$$

as the existence of the epimorphism of the quotient ring

$$R/I_1 \to R/I_2 \to \dots R/I_n$$

so this is also a categorical property, the notherian ring and Artinian ring is a Morita invariant. Finitely generation can be rephrase categorically for the for any family of submodules $\{N_i : i \in I\}$, if $\sum_{i\in I} N_i = M$ then $\sum_{j\in J} N_i = M$ for some finite subset $J \subset I$. Again the inclusion and sum preserved under categorical equivalence. Let C be a category. Then a natural transformation $\eta : \mathrm{id}_C \to \mathrm{id}_C$ consists of the following data: for every object $x \in C$, an endomorphism $\eta_x : x \to x$ such that for every morphism $f : x \to y$ in C we have

$\eta_y \circ f = f \circ \eta_x$.

Taking $x = y$ we see that eachη_x must in particular be a central element of

$$\mathrm{End}(x)$$

, so $Z(C)$ is commutative as in the group case. In particular for the category of the ring, $Z(End(R)) \cong Z(R^{op}) \cong .Z(R)$

In particular, in the context of the central simple algebra, Morita equivalence and the Brauer equivalence is coincide each other! For a central simple algebra, if two central simple algebras A, B are Brauer equivalent then $A \cong M_n(D)$ and $B \cong M_m(D)$ for some central division algebra D. We have the Morita equivalences for the matrix by $Mod(R) \ni M \to M \otimes D^n \in Mod(M_n(D))$.
If $A \cong M_n(D)$ and $B \cong M_m(E)$ where D, E are central division algebras, then $Mod(A) \cong Mod(D)$ and $Mod(B) \cong Mod(E)$. A division algebra can be recovered from its category of modules: it's the algebra of endomorphisms of the unique simple module. So $Mod(D) \cong Mod(E)$ implies $D \cong E$.

Here are some examples and problems:

Example 6.4.2. Consider the Morita equivalence $\mathbb{Z} \sim M_n(\mathbb{Z})$. Then, every $M_n(\mathbb{Z})$ module is isomorphic to $\mathbb{Z}^n \otimes_{\mathbb{Z}} M$ for an abelian group M. In particular, all f.g. (left) $M_n(\mathbb{Z})$ modules are direct sums of (columns) $C_0^{n_0} \oplus ... \oplus C_k^{n_k}$ where C_i contains the i-th component of an abelian group $M = \mathbb{Z}^{n_1} \times (\mathbb{Z}/p_1\mathbb{Z})^{n_2} \times ...(\mathbb{Z}/p_k\mathbb{Z})^{n_k}$. Moreover, every f.g. $M_n(\mathbb{Z})$-module is Noetherian.

Example 6.4.3. Morita equivalence gives us a correspondence between (left) R-ideals of R^n and (left) ideals of $M_n(R)$ by the tensor functor $M \to R^n \otimes M$, which is equivalent to considering the ideal where each row in a matrix is given by M. For instance, the left submodule of $M \subset \mathbb{Z}^2$ given by $M = \langle (1,2) \rangle$ corresponds to the left ideal $M' = M_2(\mathbb{Z}) \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$.

Problem 6.4.1 (UCLA 2021 Spring Problem 10). Let A be a ring, and P be a right A-module such that $P^n \cong A^m$ for some $m, n \geqslant 1$. Show that $S \to P \otimes_A S$ defines a bijection between the isomorphism classes of P-modules and $\mathrm{End}_A(P)$-modules.

Proof. It suffices to show that P is a progenerator for A. Indeed, since A is a direct summand of P^n, A is a generator, and since P is a direct summand of A^m, P is f.g. projective, so P is a progenerator. Thus, by Morita equivalence, there is a bijection given by the tensor functor. □

Problem 6.4.2. Given a domain R, suppose that $M_n(R)$ is a semisimple ring. Show that R is a division ring.

Proof. By Morita equivalence, semisimplicity is preserved, so R is semisimple. Thus, R is Artinian and $J(R) = 0$. But R is a domain, and an Artinian domain is a division ring, so R is a division ring. □

Throughout this section, we denote R to be the commutative ring.

There are Morita equivalence between the right $M_n(R)$-module left $M_n(R)$-module.

For the matrix ring, $M_n(R)$ there are natural bijection between left $M_n(R)$-module and the right $M_n(R)$-module by the transposition. Namely, the left $M_n(R)$-module is the column vector $R^{1\times n}$. The right $M_n(R)$-module is the row vector $R^{n\times 1}$. Given $A \in M_n(R)$ and $v \in R^n$ as a column vector, then $(Av)^T = v^T A^T$.

This transposition can be thought as the taking $Hom_R(-, R)$ for the following reason. $R^{1\times n} \cong Hom(R^{n\times 1}, R)$ because homomorphism

$$\begin{pmatrix} * & * & * \end{pmatrix}$$

$$\begin{pmatrix} * \\ * \\ * \end{pmatrix}$$

We gave $R^{n\times 1}$ structure of left $M_n(R)$ module and right R module, we have left R-module structure and right-$M_n(R)$ module structure for the $R^{1\times n}$.

Right ideal of $M_n(R)$ and right R-submodule R^n are one to one correspondence in the following way. Given the right ideal of $M_n(M)$ we can find a module of R^n by the set spanned by

$$span\{Xe_i | X \in I\}$$

where e_i are the column vector of R^n everywhere 0 except for the i-th component. On the other hand, given the right R^n module K, we can find the ideal by

$$\{X | \text{for all } v \in R^n, Xv \in K\}.$$

We can easily check that composition of this maps are identity.

One can check $R^{n\times 1} \otimes_R R^{1\times n} \cong M_n(R)$ as a bimodule(this can be seen from the exhibiting basis.

7 Group Theory