Note for Algebra I

lumi

General Term

Definition 1. Let A be some algebraic structure.
A is *simple* if there is no proper non-trivial normal substructure.

Module Theory

Lemma 1. *If R is commutative, $\mathrm{Hom}_R(M, N)$ is an R-module.*

Definition 2. $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ is an *endomorphism ring.*

Definition 3. Annihilator $\mathrm{ann}(m) = \{r \in R \mid rm = 0\}$

Lemma 2. $R/\mathrm{ann}(m) \simeq Rm$

Theorem 1. *There is an abelian group denoted by $M \otimes_R N$ with an$R$-balanced map $\iota : M \times N \to M \otimes_R N$ with the following universal property: for any R-balanced map $\varphi : M \times N \to L$ for some $L \in (\mathrm{Ab})$, there is a unique group homomorphism $\tilde{\varphi} : M \otimes_R N \to L$ such that*

$$\begin{tikzcd}
M \times N \arrow[rr, "\varphi"] \arrow[dr, "\iota"'] & & L \\
& M \otimes_R N \arrow[ur, "\tilde{\varphi}"'] &
\end{tikzcd}$$

commutes

Theorem 2. *$M \otimes_R N \simeq M \times N/Q$ such that Q is generated by*

- $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$
- $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$
- $(mr, n) - (m, rn)$

Example. $R/I \otimes_R R/J = R/(I + j)$

Example. $R[t_1, \cdots, t_r] = R \otimes_k k[t_1, \cdots, t_r]$

Example. $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$

Theorem 3. *For a commutative rings with unity, the tensor product is a push-out such that:*

$$\begin{tikzcd}
R \arrow[r] \arrow[d] & R_1 \arrow[d] \\
R_2 \arrow[r] & R_1 \otimes_R R_2
\end{tikzcd}$$

Theorem 4. *For $\phi : M \to M'$ and $\psi : N \to N'$, there is a unique homomorphism (of groups)*

$$\phi \otimes \psi : M \otimes_R N \to M' \otimes_R N'$$

such that $(\phi \otimes \psi)(m \otimes n) = \phi(m) \otimes \psi(n)$.

Theorem 5. *There is a natural isomorphism:*

$$(M \otimes_R N) \otimes_T L \simeq M \otimes_R (N \otimes_T L)$$

Theorem 6.

$$(\bigoplus_i M_i) \otimes_R N \simeq \bigoplus_i (M_i \otimes_R N)$$

Theorem 7. *Given an R-algebra $R \to S$,*

$$S \otimes_R R^{\otimes n} \simeq S^{\oplus n}$$

Theorem 8.

$$R^m \otimes_R R^n = R^{mn}$$

Definition 4. Let R be a ring with unity, and M be a non-zero R-module.

1. M is irreducible (or simple), if there are no proper non-trivial submodule of M. Otherwise, M is reducible.

2. M is indecomposable if M is not of the form $M_1 \oplus M_2$ for non-zero submodules $M_1, M_2 \subseteq M$. Otherwise, M is called decomposable.

3. M is completely reducible if M is a direct sum of irreducible submodules.

4. Each direct summand of irreducible decomposition of M is called a constituent of M.

Theorem 9. *If M is irreducible, it's indecomposable and completely reducible.*

Homology

Definition 5. $A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ of R-modules is called exact at B if $\ker \psi = \operatorname{im} \varphi$.

Definition 6. $A_{i+1} \xrightarrow{\varphi_{i+1}} A_i \xrightarrow{\varphi_i} A_{i-1}$ is called a complex of R-modules, if $\varphi_i \circ \varphi_{i+1} = 0$. The i-th homology is $H_i(A_\bullet) = \ker \varphi_i / \operatorname{im} \varphi_{i+1}$. $A_\bullet$ is exact if all homology is zero.

Theorem 10. $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ *is (1) exact at A iff φ is injective, (2) exact at B iff ψ is surjective.*

Definition 7. For $C \simeq A \oplus B$,

$$0 \to A \to C \to B \to 0$$

is a short exact sequence.

Theorem 11. *For $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$, TFAE: (1) it's split; (2) there is a homomorphism $s : C \to B$ such that $\psi \circ s = \mathrm{Id}_C$; (3) there is a homomorphism $p : B \to A$ such that $p \circ \varphi = \mathrm{Id}_A$;*

Theorem 12. *(Short Five Lemma) For a commutative diagram with exact rows:*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "f"] & B \arrow[r] \arrow[d, "g"] & C \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 0
\end{tikzcd}$$

If f and h are injective/surjective/isomorphisms, then so is g.

Theorem 13. *(Horseshoe Lemma for Projective Resolution) For given s.e.s $0 \to M' \to M \to M''$, projective resolutions $P'_\bullet \to M'$ and $P''_\bullet \to M''$, there is a projective resolution $P_\bullet \to M$ and a double complex*

$$0 \to P'_\bullet \to P_\bullet \to P''_\bullet \to 0$$

such that each rows and columns are exact.

Theorem 14. *(Horseshoe Lemma for InjectiveResolution) For given s.e.s $0 \to M' \to M \to M''$, projective resolutions $M' \to I'^\bullet$ and $M'' \to I''^\bullet$, there is a projective resolution $M \to I^\bullet$ and a double complex*

$$0 \to I'^\bullet \to I^\bullet \to I''^\bullet \to 0$$

such that each rows and columns are exact.

Theorem 15. *(Snake Lemma) Suppose we have a commutative diagram with exact rows:*

$$\begin{tikzcd}
 & A_1 \arrow[r, "\alpha"] \arrow[d, "f"] & A_2 \arrow[r, "\beta"] \arrow[d, "g"] & A_3 \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & B_1 \arrow[r, "\gamma"] & B_2 \arrow[r, "\delta"] & B_3 &
\end{tikzcd}$$

Then, there is a natural homomorphism ∂ and an exact sequence

$$\ker f \to \ker g \to \ker h \xrightarrow{\partial} \operatorname{coker} f \to \operatorname{coker} g \to \operatorname{coker} h$$

If α is injective, so is $\ker f \to \ker g$. If δ is injective, so is $\operatorname{coker} g \to \operatorname{coker} h$.

Theorem 16. *Let $0 \to A_\bullet \to B_\bullet \to C_\bullet \to 0$ be a s.e.s of complexes of R-modules. Then there is a long exact sequence*

$$\begin{tikzcd}
\cdots \arrow[r] & H_n(A) \arrow[r] & H_n(B) \arrow[r] & H_n(C) \arrow[dll, "\partial"'] & \\
 & H_{n-1}(A) \arrow[r] & H_{n-1}(B) \arrow[r] & H_{n-1}(C) \arrow[r] & \cdots
\end{tikzcd}$$

Theorem 17. $\operatorname{Hom}_R(D, -)$ *and* $\operatorname{Hom}_R(-, D)$ *are left exact.*

Example. $\operatorname{Hom}_R(D, -)$ is not exact, beacuse of $0 \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to \mathbb{Z}/n \to 0$.

Theorem 18. *For a ring R and an R-module P, TFAE,*

- $\operatorname{Hom}_R(P, -)$ *is exact,*
- *P is a projective R-module,*

- *For every s.e.s* $0 \to L \to M \to P \to 0$*, this splits,*
- P *is a direct summand of a free* R*-module.*

Definition 8. For projective $P_\bullet$, exact $P_\bullet \xrightarrow{\epsilon} M$ is a projective resolution of M.

Theorem 19. *For a ring* R *and an* R*-module* Q*, TFAE,*

- $\mathrm{Hom}_R(-, Q)$ *is exact,*
- Q *is an injective* R*-module,*
- *For any s.e.s* $0 \to Q \to M \to N \to 0$ *is split.*

Theorem 20. *(Theorem (B)) Let* Q *be an* R*-module. Then there is an injective homomorphism* $Q \rightarrowtail I$ *such that* I *is an injective* R*-module.*

Theorem 21. *(Theorem (C))* $\prod_i Q_i$ *is injective iff each* Q_i *is injective.*

Theorem 22. *(Baer Criterion)* Q *is injective, iff, for all each ideal* $I \subseteq R$ *and each* R*-module homomorphism* $G : I \to Q$*, it extends to* $\tilde{g} : R \to Q$*.*

Corollary 1. *Let* R *be a PID. Then* Q *is injective iff for each* $r \in R \setminus \{0\}$*, we have* $rQ = Q$*.*

Lemma 3. *Let* J *be an abelian group and* R *be a ring with unity. Then,* $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ *is a left* R*-module.*

Theorem 23. *(Theorem (D)) Let* J *be a divisible abelian group, and* R *be a ring with unity. Then,* $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ *is an injective* R*-module.*

Theorem 24. *A tensor functor,* $D \otimes_R -$*, is right exact. In the same sense,* $- \otimes_R D$ *is right exact.*

Example. A tensor product is not exact, because for $D = \mathbb{Z}/n$, and $0 \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to \mathbb{Z}/n \to 0$.

Definition 9. D is *flat* right R-module, if a tensor functor $D \otimes_R -$ is exact.
D is *flat* left R-module, if a tensor functor $- \otimes_R D$ is exact.

Theorem 25. *(Adjunction) Let* R, S *be rings with unity,* A *be a right* R*-module,* B *be* (R, S)*-bimodule,* C *be a right* S*-module. Then, there is a natural isomorphism of abelian groups:*

$$\mathrm{Hom}_S(A \otimes_R B, C) \to \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$$

where $A \otimes_R B$ *is seen as a right* S*-module and* $\mathrm{Hom}_S(B, C)$ *which is a right* R*-module.*

Note. $\varphi : A \otimes_R B \to C$ induces $\psi : A \to \mathrm{Hom}_S(B, C)$ such that $\psi(a) = \psi_a$ and $\psi_a = \varphi(a \otimes -)$.

Note. $\psi : A \to \mathrm{Hom}_S(B, C)$ defines $\varphi \in \mathrm{Hom}_S(A \otimes_R B, C)$ given by $\varphi(a \otimes b) = \psi(a)(b)$.

Theorem 26. *For a commutative ring with unity* R*, in* $R - \mathrm{Mod}$*,*

$$\textit{Free} \Rightarrow \textit{Projective} \Rightarrow \textit{Flat} \Rightarrow \textit{Torsion-Free}$$

Example. 0 is free. Thus, it's projective, flat, and torsion-free.

Theorem 27. *For a commutative ring* R *with unity,* P, Q *are projective* R*-modules, then* $P \otimes_R Q$ *is also projective.*

Theorem 28. R*-modules are enough projective and enough injective.*

Theorem 29. *For complexes of R-modules $A_\bullet$ and $B_\bullet$, $f_\bullet : A_\bullet \to B_\bullet$ is a chain map such that the following diagram commutes:*

$$\begin{tikzcd} \cdots \arrow[r] & A_{n+1} \arrow[r] \arrow[d, "f_{n+1}"] & A_n \arrow[r] \arrow[d, "f_n"] & A_{n-1} \arrow[r] \arrow[d, "f_{n-1}"] & \cdots \\ \cdots \arrow[r] & B_{n+1} \arrow[r] & B_n \arrow[r] & B_{n-1} \arrow[r] & \cdots \end{tikzcd}$$

Theorem 30. *f_n induces an induced homomorphism $f_n : H_n(A_\bullet) \to H_n(B_\bullet)$.*

Definition 10. $f_\bullet$ is a quasi isomorphism if induced $f_\bullet$ into homologies is isomorphisms.

Definition 11. For two complexes $A_\bullet$ and $B_\bullet$, they are *quasi-isomorphic*, if there is a zig-zag of complexes and quasi-isomorphism $A_\bullet \leftarrow C^0 \to C^1 \leftarrow C^2 \to \cdots \to B_\bullet$.

Definition 12. $\mathrm{Kom}(R)$ is the category of all complexes of R-modules, where objects are complexes and morphisms are chain maps. $\mathrm{Kom}^+(R)$ is bounded below, $\mathrm{Kom}^-(R)$ is bounded below, and $\mathrm{Kom}^b(R)$ is bounded below.

Definition 13. Let R be a ring with unity, $f_\bullet, g_\bullet : A_\bullet \to B_\bullet$ be two chain maps. If there are R-module homomorphisms $s = \{s_n \mid A_n \to B_{n+1}\}$ such that $f - g = sd + ds$.

If there is a (chain) homotopy between $f$and g, they are (chain) homotopic. $f \sim^s g$.

Theorem 31. *If f, g are chain homotopic, then, f_n, g_n induced into homologies are equal.*

Definition 14. If chain map is homotopic to the zero map, f is null homotopic.

Definition 15. f is a chain homotopy equivalence if there is a chain map g such that $g \circ f$ and $f \circ g$ are identity maps.

Theorem 32. *If f is a chain homotomy equivalence, it's a quasi-isomorphism.*

Theorem 33. *If $f_1, f_2 : A_\bullet \to B_\bullet$ and $g_1, g_2 : B_\bullet \to C_\bullet$ are chain homotopic chain maps, $g_1 \circ f_1$ and $g_2 \circ f_2$ are chain homotopic.*

Definition 16. $K(R)$ is the category such that: $\mathrm{Ob}(K(R))$ is the complexes of R-modules, $\mathrm{Hom}(K(R))$ is $\mathrm{Hom}_{K(R)}(A_\bullet, B_\bullet) = \mathrm{Hom}_{\mathrm{Kom}(R)}(A_\bullet, B_\bullet)/\sim$, where $\sim$ is the chain homotopy.

Definition 17. $D(R)$ is the *derived category* such that: $\mathrm{Ob}(K(R))$ is the complexes of R-modules, $\mathrm{Hom}(K(R))$ is $\mathrm{Hom}_{D(R)}(A_\bullet, B_\bullet) = \mathrm{Hom}_{\mathrm{Kom}(R)}(A_\bullet, B_\bullet)/\sim_{q.iso}$, where $\sim$ is the chain homotopy.

Theorem 34. *(Pseudo-universal Property) Let R be a ring with unity, M, N be R-modules. Let $P_\bullet \to M$ and $Q_\bullet \to N$ be projective resolutions, and let $f_{-1} : M \to N$ be any R-module homomorphism. Then, there is a chain map $f_\bullet : P_\bullet \to Q_\bullet$ which lifts f_{-1}. $f_\bullet$ is unique up to chain homotopy.*

Theorem 35. *(Pseudo-universal Property) Two projective resolutions of R-module M are unique un to chain homotopy equivalence.*

Definition 18. Projective resolution of $M_\bullet$ is a projective chain complex $P_\bullet$ if there is a quasi-isomorphism between $M_\bullet$ and $P_\bullet$.

Theorem 36. *(HW5-Problem 2, 5) For bounded above complex $M_\bullet$, there is a projective resolution of $M_\bullet$.*

For bounded below complex $M^\bullet$, there is an injective resolution of $M^\bullet$.

Definition 19. Let $P_\bullet \to M$ be a projective resolution. $\mathrm{Tor}_i^R(N, M) := H_i(N \otimes_R P_\bullet)$.

Let $N \to I^\bullet$ be a projective resolution. $\mathrm{tor}_i^R(N, M) := H^i(I^\bullet \otimes_R M)$.

Lemma 4. *$\mathrm{Tor}_i^R(N, M)$ is independent of the choice of a projective resolution $P_\bullet \to M$ up to isomorphism. $\mathrm{tor}_i^R(N, M)$ is independent of the choice of a injective resolution $N \to I^\bullet$ up to isomorphism.*

Theorem 37. *If N, M are projective, Tor_i^R are 0 for $i \geq 1$. In the same way, if N, M are injective, tor_i^R are 0 for $i \geq 1$.*

Theorem 38. $\mathrm{Tor}_i^R(N, M) \simeq \mathrm{tor}_i^R(N, M)$

Definition 20. Let $A_\bullet$ and $B_\bullet$ be complexes. $\mathrm{Tor}(A \otimes B) = T_\bullet = \{T_n\}$ is a total complex of A and B where $T_n = \bigoplus_{i+j=n} A_i \otimes B_j$.

Theorem 39. *(HW5-P6) For a projective resolution $Q_\bullet \to N$ and $P_\bullet \to M$, there is a natural quasi-isomorphism $\mathrm{Tot}(P \otimes Q)_\bullet \to Q_\bullet \otimes_R M$.*

Theorem 40. *Let $0 \to N_1 \to N_2 \to N_3 \to 0$ be a s.e.s of R-modules, and $M \in \mathrm{Ob}(R-\mathrm{Mod})$. Then, there is a long exact sequence*

$$\begin{tikzcd}
\cdots \arrow[r] & \mathrm{tor}_n(N_1, M) \arrow[r] & \mathrm{tor}_n(N_2, M) \arrow[r] & \mathrm{tor}_n(N_3, M) \arrow[dll, "\partial"'] \\
& \mathrm{tor}_{n-1}(N_1, M) \arrow[r] & \mathrm{tor}_{n-1}(N_2, M) \arrow[r] & \mathrm{tor}_{n-1}(N_3, M) \arrow[r] & \cdots
\end{tikzcd}$$

Definition 21. Let R be a ring with unity, M, N be left R-modules. Let $N \to I^\bullet$ be an injective resolution. $\mathrm{Ext}_R^n(M, N) = H^n(\mathrm{Hom}_R(M, I^\bullet))$.

Let $I_\bullet \to M$ be a projective resolution. $\mathrm{ext}_R^n(M, N) = H^n(\mathrm{Hom}_R(P_\bullet, N))$.

Theorem 41. *Ext_R^n is independent of the choice of an injective resolution up to isomorphism. ext_R^n is independent of the choice of a projective resolution up to isomorphism.*

Theorem 42. $\mathrm{Ext}_R^0(M, N) \simeq \mathrm{Hom}_R(M, N) \simeq \mathrm{ext}_R^0(M, N)$.

Theorem 43. *If N is injective and $n > 0$, then $\mathrm{Ext}_R^n(M, N) = 0$.*

If M is projective and $n > 0$, then $\mathrm{ext}_R^n(M, N) = 0$.

Theorem 44. *Let $0 \to N_1 \to N_2 \to N_3 \to 0$ be a s.e.s of R-modules, and $M \in \mathrm{Ob}(R-\mathrm{Mod})$. Then, there is a long exact sequence*

$$\begin{tikzcd}
\cdots \arrow[r] & \mathrm{Ext}^n(M, N_1) \arrow[r] & \mathrm{Ext}^n(M, N_2) \arrow[r] & \mathrm{Ext}^n(M, N_3) \arrow[dll, "\partial"'] \\
& \mathrm{Ext}^{n+1}(M, N_1) \arrow[r] & \mathrm{Ext}^{n+1}(M, N_2) \arrow[r] & \mathrm{Ext}^{n+1}(M, N_3) \arrow[r] & \cdots
\end{tikzcd}$$

Theorem 45. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a s.e.s of R-modules, and $M \in \mathrm{Ob}(R-\mathrm{Mod})$. Then, there is a long exact sequence*

$$\begin{tikzcd}
\cdots \arrow[r] & \mathrm{ext}^n(M_3, N) \arrow[r] & \mathrm{ext}^n(M_2, N) \arrow[r] & \mathrm{ext}^n(M_1, N) \arrow[dll, "\partial"'] \\
& \mathrm{ext}^{n+1}(M_3, N) \arrow[r] & \mathrm{ext}^{n+1}(M_2, N) \arrow[r] & \mathrm{ext}^{n+1}(M_1, N) \arrow[r] & \cdots
\end{tikzcd}$$

Theorem 46. $\mathrm{Ext}_R^n(M, N) \simeq \mathrm{ext}_R^n(M, N)$.

Definition 22. An *extension* of M by N is a s.e.s of R-modules

$$0 \to N \to T \to M \to 0$$

. If the s.e.s splits, it's *the trivial extension.*

Definition 23. If T_1, T_2 are two extensions of M by N and there is a homomorhpism $T_1 \to T_2$, it's an isomorphism by the Short Five Lemma, and T_1 and T_2 are said to be *equivalent.*

Definition 24. $\operatorname{Ext}_R(M, N)$ be the set of equivalence classes of extensions of M by N.

Lemma 5. *Let* $e := [0 \to N \to T \to M \to 0] \in \operatorname{Ext}_R(M, N)$*. Then there is a well-defined class* $\delta(e) \in \operatorname{Ext}^1_R(M, N)$*.*

Lemma 6. *Let* $e = [0 \to N \to T \to M \to 0] \in \operatorname{Ext}_R(M, N)$*. e is a split exact sequence iff* $\delta(e) = 0$*.*

Theorem 47. *The map* $\delta : \operatorname{Ext}_R(M, N) \to \operatorname{Ext}^1_R(M, N)$ *is bijective.*

Definition 25. Let $e_i : 0 \to N \to T_i \to M \to 0$ for $i = 1, 2$. Consider the pull-back T' of $T_1 \to M \leftarrow T_2$, i.e. $T' \subseteq T_1 \times T_2$ consisting of (t_1, t_2) whose images in M coincide. Let $D \subseteq T'$ be generated by $(-n, n)$ for $n \in N$, and let $T := T'/D$. This gies a s.e.s $e : 0 \to N \to T \to M \to 0$, which is called *the Baer sum of* e_1 *and* e_2*.*

Theorem 48. $\operatorname{Ext}_R(M, N)$ *and the Baer Sum give a group structure. Furthermore,* $\delta : \operatorname{Ext}_R(M, N) \to \operatorname{Ext}^1_R(M, N)$ *is a group homomorphism.*

Definition 26. An *n-extension of M by N* is an exact sequence of the form

$$0 \to N \to T_n \to \cdots \to T_1 \to M$$

Definition 27. If there is chain map $f_\bullet$ between extension $T_\bullet$, $T'_\bullet$ of M by N, it's an equivalence. Also, the class of this equivalence give $\operatorname{Ext}^{(n)}_R(M, N)$, which is called *the Yoneda n-Extension*

Theorem 49. *The Yoneda n-Extension with a higher Baer sum is isomorphic to* Ext^n_R*.*

Definition 28. Let $P_\bullet \to M$ be a projective resolution.

Then, if there is some $N \geq 0$ such that $P_n = 0$ for every $n > N$, *the length of the projective resolution is less or equal to N.*

If no such N, the length is infinite.

The projective dimension $\operatorname{pd}_R M$ is the smallest length of such projective resolutions.

Theorem 50. *(HW8-P1)*

- $\operatorname{pd}_k V = 0$ *for a field k.*
- $\operatorname{pd}_R M \leq 1$ *for PID R and a finitely generated R-module M.*

Tensor Algebra

Definition 29. Let $T^0_R(M) := R$ and for $k \geq 1$, let

$$T^k_R(M) = T^k(M) := M \otimes_R \cdots \otimes_R M$$

Let $T_R(M) = T(M) := \bigoplus_{k \geq 0} T^k(M)$. We have the associative $\otimes : T^r(M) \otimes_R T^s(M) \to T^{r+s}(M)$. This $(T_R(M), +, \otimes, \cdot)$ is called *the tensor algebra of M over R.*

Theorem 51. *(Universal Property of Tensor Algebra) Let R be a commutative ring with 1, A be any R-algebra with a given $\varphi : M \to A$ where A is an R-module homomorphism. Then, there exists a unique R-algebra homomorhpism ψ such that the diagram*

$$\begin{tikzcd} M \arrow[rr, "\varphi"] \arrow[dr, "\mathrm{Id}"'] & & A \\ & T(M) \arrow[ur, "\psi"'] & \end{tikzcd}$$

where $\mathrm{Id} : M \to M = T^1(M)$ *is the identity.*

Definition 30. R: comm. ring with 1, M: R-module, $T(M)$: tensor algebra. Let $C(M) \subseteq T(M)$ be the two sided ideal generated by elements of the form $m_1 \otimes m_2 - m_2 \otimes m_1$. Let

$$S(M) = \mathrm{Sym}(M) := T(M)/C(M)$$

Let $S^k(M) = \mathrm{Sym}^k(M)$ be the image of $T^k(M)$.

$\mathrm{Sym}(M)$ is called *the symmetric algebra of M over R.*

Example. For $M = R^n$, the free R-module of rank n, $\mathrm{Sym}(M) \simeq R[t_1, \cdots, t_n]$ where $\mathrm{Sym}^k(M)$ as an R-module is spanned by th emonomials of degree k, and free of rank $\binom{k+n-1}{n-1}$.

Theorem 52. $\mathrm{Sym}(M)$ *satisfies the universal property for* commutative *R-algebra A.*

Definition 31. R: comm. ring with 1, M: R-module, $T(M)$: tensor algebra. Let $A(M) \subseteq T(M)$ be the two sided ideal generated by elements of the form $m \otimes m$. Let

$$\wedge(M) = T(M)/A(M)$$

Let $\wedge^k(M)$ be the image of $T^k(M)$.

$\wedge(M)$ is called *the exterior algebra of M over R.*

Lemma 7. *When $m, m' \in M$, $m \wedge m' = -m' \wedge m$.*

Theorem 53. $\wedge^k(M)$ *satisfies the universal property with the alternating R-multilinear $\varphi : M \times \cdots \times M \to N$.*

Example. Let M be a free r-module of rank n. Then $\wedge^k(M)$ is free of rank $\binom{n}{k}$. In particular, $\wedge(M)$ is in fact "bounded above" in that

$$\wedge(M) = \bigoplus_{k=0}^{n} \wedge^k(M)$$

Definition 32. (Lie Algebra) An F-vector space L is called a *Lie algebra*, if there is an alternating ($[x, x] = 0$) bilinear map

$$[-, -] : L \times L \to L$$

satisfying the Jacobi identity:

$$[x, [y, z]] + [z, [x, y]] + [y, [z, x]] = 0$$

Example. Let L be an F-algebra. Take $[x, y] = xy - yx$. Then, L gives a Lie algebra.

Theorem 54. *(Universal Envelopping Algebra) Let L be a Lie algebra over F and let A be an associative F-algebra with the induced Lie algebra structure. Let $\phi : L \to A$ be a Lie algebra homomorphism, i.e. $\phi([x, y]) = \phi(x)\phi(y) - \phi(y)\phi(x)$ for $x, y \in L$.*

Then there is an F-algebra $U(L)$ together with an F-linear map $i : L \to U(L)$ such that there is a unique F-algebra homomorphism $\psi : U(L) \to A$ such that the following commutes:

$$\begin{tikzcd} L \arrow[rr, "\phi"] \arrow[dr, "i"'] & & A \\ & U(L) \arrow[ur, "\psi"'] & \end{tikzcd}$$

This is constructed by taking the two-sided ideal $I(L)$ generated by elements of the form $x \otimes y - y \otimes x - [x, y]$, and take $U(L) = T(L)/I(L)$.

Theorem 55. *(Poincaré-Birkhoff-Witt) Let F be a field, L be an F-Lie algebra with a basis $\mathcal{B}$. Give a well-ordering on $\mathcal{B}$.*

A canonical monomial over $\mathcal{B}$ is a sequence $(x_1, \cdots, x_r)$ with $x_1 \le \cdots \le x_r$, $x_i \in \mathcal{B}$. For the natural map $i : L \to U(L)$, define $i(x_1, \cdots, x_r) := i(x_1) \cdots i(x_r)$.

Then i is injective on the set of all canonical monomials, and the images form an F-basis of $U(L)$.

Corollary 2. *$i : L \to U(L)$ is injective.*

Linear Algebra

Definition 33. Let R be an integral domain, M be an R-module. The *rank of M over R* is the maximum cardinality of R-linearly independent elements of M.

Theorem 56. *(A) Let R be a PID, M be a free R-module of rank n, and $N \subseteq M$. Then (1) N is free of rank $m \le n$; (2) We can find a basis $y_1, \cdots, y_n \in M$ such that for some $a_1 \mid a_2 \mid \cdots \mid a_m$, $a_1 y_1, \cdots, a_m y_m \in N$ and they form a basis of N.*

Theorem 57. *(Fundamental Theorem for Finitely Generated Modules over PID)*

Let R be a PID, M be a finitely generated R-modules. Then,

$$M \simeq R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$

for some $a_i \in R$ such that $a_1 \mid a_2 \mid \cdots \mid a_m$. The number r is unique and $a_1, \cdots, a_m$ are uniquely decided up to units in R.

Corollary 3. *Fundamental Theorem of Finitely Generated Abelian Group holds.*

Corollary 4. *For $R = k[t]$, FTFGMPID gives the Cyclic Decomposition Theorem.*

Representation

Definition 34. Let G be a group, F be a field, V be an F-vector space.

1. A *(linear) representation of G (over F)* is a group homomorphism $\varphi : G \to \mathrm{GL}(V)$.

   The *degree* of the representation if $\dim_F(V)$.

2. A *matrix representation* of G is a homomorphism $G \to \mathrm{GL}_m(V)$.

   When $\dim_F V = m$, we have $\mathrm{GL}(V) \simeq \mathrm{GL}_m(V)$, so we generally do not distinguish these two, unless we have reason to do so.

3. A representation $G \to \mathrm{GL}(V)$ is *faithful* if it is injective.

Definition 35. Let G be a group and R be a ring. RG is the group ring, where (1) each element is in a form of $\sum_{g\in G} \alpha_g \cdot g$; (2) addition is sum term-by-term; (3) multiplication is sum of multiplication of mult. of coefficients and mult. of G-terms.

Lemma 8. *Let V be a set. V is an FG-module iff V is an F-vector space and there is a group homomorphism $\phi : G \to \mathrm{GL}(V)$.*

Definition 36. Let V, W be representations of G over F. A morphism of representation G, $\phi : V \to W$, is an FG-module homomorphism. Two representations V, W are *equivalent* if they are isomorphic as FG-modules.

Corollary 5. *The representations of G over F form a category $G - \mathrm{Rep}/F$ and there is a natural equivalence of categories:*

$$FG - \mathrm{Mod} \Leftrightarrow G - \mathrm{Rep}/F$$

Definition 37. Let G be a group. Let $V = FG$ with the left FG-module structure.

The induced representation $\phi : G \to \mathrm{GL}(FG)$ is called the *regular representation of G*.

Theorem 58. *Regular representations are faithful.*

Theorem 59. *(Maschke) Let G be a finite group, F be a field such that* $\mathrm{char}(F) = 0$ *or* $\mathrm{char}(F) = p > 0$ *with $p \nmid |G|$.*

Let V be an FG-module and $U \subseteq V$ be any FG-submodule. Then there is an FG-submodule $W \subseteq V$ such that

$$V \simeq U \oplus W$$

as FG-modules.

Theorem 60. *(Wedderburn-Artin) Let R be a ring with 1. Then, TFAE*

1. *R is a* semi-simple ring.
2. *R is Artinian and its Jacobson radical is zero.*
3. *Every R-module is projective.*
4. *Every R-module is injective.*
5. *Every R-module is completely reducible.*
6. *The ring R considered as a left R-module is a direct sum $R = L_1 \oplus \cdots \oplus L_n$ of simple R-modules L_i, with $L_i = Re_i$, such that $e_i e_j = \delta_{ij} e_i$ and $\sum e_i = 1$.*
7. *As rings, R is isomorphic to $R_1 \times \cdots \times R_r$ where $R_j = M_{n_j}(D_j)$, for some division ring D_j. The integer r, n_j and the ring D_j are unique.*

Note, semi-simple ring are Artinian and Noetherian.

Corollary 6. *(Corollary of Maschke's) F, G, FG be as before, and M be a finitely generated FG-module. Then, M is completely reducible. i.e. the group ring FG is a semi-simple ring.*

Theorem 61. *(Schur's Lemma) Let R be a non-zero ring with 1. Let M, N be simple R-modules. Let $\varphi : M \to N$ be an R-module homomorphism. Then, either φ is 0 or an isomorphism.*

Corollary 7. *(Special Case of Schur's Lemma) If M is a simple R-module, then* $\mathrm{Hom}_R(M, M) = \mathrm{End}_R(M)$ *is a division ring.*

Theorem 62. *Let D be a division ring and $R = M_n(D)$. Then R is a simple ring, i.e. the only two-sided ideals of R are 0 and R.*

Theorem 63. *Let D be a division ring and $R = M_n(D)$. Then $Z(R)$, the center of R is $\{\alpha I_n \mid \alpha \in Z(D)\}$, where I_n is the n-by-n identity matrix.*

Theorem 64. *Let D be a division ring and $R = M_n(D)$. Let $e_i = E_{ii}$. Then,*

- *$e_i e_j = \delta_{ij} e_i$ and $\sum e_i = 1$.*
- *Let $L_i = Re_i$. Then they are simple left R-modules.*
- *Every simple left R-module is isomorphic to L_1.*
- *As a left R-module, $R = L_1 \oplus \cdots \oplus L_n$.*

Theorem 65. *Let D be a division ring, which is a finite dimension vector space over a field F with $F \subseteq Z(D)$, and $F = \overline{F}$. Then, $D = F$.*

Theorem 66. *Let G be a finite group. Then for some $n_1, \cdots, n_r$ and $r \geq 1$, we have*

$$\mathbb{C}G \simeq M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$$

Corollary 8. $|G| = \sum_{i=1}^{r} n_i^2$

Theorem 67. *$\mathbb{C}G$ has exactly r distinct isomorphism types of irreducible modules, i.e. there are exactly r non-equivalent irreducible representations of G. Here, each $M_{n_i}(\mathbb{C})$ decomposes into a direct sum of n_i isomorphic irreducible modules.*

Theorem 68. *Let G be a finite group. In the decomposition*

$$\mathbb{C}G \simeq M_{n_1}(\mathbb{C}) \times M_{n_r}(\mathbb{C})$$

into simple rings, the number r is equal to the number of conjugacy classes of G.

Corollary 9. *When A is a finite abelian group, every irreducible representation over $\mathbb{C}$ is of degree* 1 *(or 1-dimensional), and A has exactly $|A|$ inequivalent irreducible representations.*

Theorem 69. *Let G be a finite group. Then the number of inequivalent irreducible representations of degree 1 is $|G/[G, G]|$.*

Definition 38. Let G be a group and F be a fixed field.

A *class function* $\varphi : G \to F$ is a set-function, constant on conjugacy classes. i.e. $\varphi(gxg^{-1}) = \varphi(x)$ for every $g, x \in G$.

Given a representation $\varphi : G \to \mathrm{GL}(V)$, the *character of* φ is the set-function $\chi : G \to F$ such that $\chi(g) = \mathrm{Tr}\,\varphi(g)$.

Definition 39. Let G be a group, F be a fixed field, $\varphi : G \to \mathrm{GL}(V)$ be a representation, and $\chi = \mathrm{Tr}\,\varphi$ be the character of φ.

χ is irreducible if φ is an irreducible representation.

χ is reducible if φ is an reducible representation.

Definition 40. The character of the trivial representation is the *principal character*.

Theorem 70. *For a representation $\varphi : G \to \mathrm{GL}(V)$ and $\chi = \mathrm{Tr}\,\varphi$, χ is a class function.*

Lemma 9. *For a representation $\varphi : G \to \mathrm{GL}(V)$ and $\chi = \mathrm{Tr}\,\varphi$, $\chi(1_G) = \dim_F V = \deg \varphi$.*

Theorem 71. *Every character of linear representation of group, $\chi : G \to F$, can be extended F-linearly to $\chi : FG \to F$.*

Theorem 72. *For irreducible modules M_i with the irreducible character χ_i and*

$$M \simeq M_1^{\bigoplus a_1} \oplus \cdots \oplus M_r^{\bigoplus a_r}$$

then, the character χ of M is

$$\chi = \sum_i a_i \chi_i$$

Theorem 73. *Let G be a finite group. Let M, N be two finite dimensional representations of G. Let χ, ψ be their characters. Then, $M \simeq N$ as $\mathbb{C}G$-modules iff $\chi = \psi$.*

Corollary 10. *For a given finite group G,*

- *Irrducible characters χ_i completely determine all finite dimensional representations of G up to equivalence.*
- *Irreducible characters completely determine all finitely generated $\mathbb{C}G$-modules up to isomorphism.*
- *There is an one-to-one correspondence between each set of irreducible characters and each irreducible $\mathbb{C}G$-module.*

Definition 41. Let $\mathcal{F}$ be the vector space of $\mathbb{C}$-valued class functions on G.

Definition 42. s_i is a step function such that

$$s_i(K_j) = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$

Proposition 1. *Irreducible characters χ_i are in $\mathcal{F}$. e_i are also in $\mathcal{F}$. Since e_i are linearly independent and span $\mathcal{F}$, $\dim_{\mathbb{C}} \mathcal{F} = r$. where r is the number of distinct irreducible characters.*

Theorem 74. *The irreducible characters $\chi_1, \cdots, \chi_r \in \mathcal{F}$ are linearly independent. In particular $\chi_1, \cdots, \chi_r$ form a basis for $\mathcal{F}$.*

Definition 43. Define a hermitian inner product on $\mathcal{F}$ as follows: for $\theta, \psi \in \mathcal{F}$, define

$$(\theta, \psi) := \frac{1}{|G|} \sum_{g \in G} \theta(g)\overline{\psi(g)}$$

Theorem 75. *(1st Schur Orthogonality Theorem) Let G be a finite group, and $\chi_1, \cdots, \chi_r$ be irreducible characters of G. Then $(\chi_i, \chi_j) = \delta_{ij}$.*

i.e. $\{\chi_i\}_i$ is an orthonormal basis of the space of class functions $\mathcal{F}$.

In particular, for $\theta \in \mathcal{F}$,

$$\theta = \sum_{i=1}^{r} (\theta, \chi_i)\chi_i$$

Lemma 10. *In $\mathbb{C}G$, we have*

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g$$

Lemma 11. *Let $\psi : G \to \mathbb{C}$ be any character. Then,*

- *$\psi(x)$ is a sum of roots of unity.*
- *$\psi(x^{-1}) = \overline{\psi(x)}$ for all $x \in G$.*

Theorem 76. *Let $\varphi : G \to \mathrm{GL}(V)$ be a representation for a finite dimensional vector space V. Let $\{v_1, \cdots, v_n\}$ be a basis of V and let $\{v_1^*, \cdots, v_n^*\}$ be its dual basis.*

Then $\mathrm{Tr}\,\varphi(g) = \sum_{i=1}^n v_i^*(g \cdot v_i)$.

Definition 44. Let V be a representation of G. We can define the dual representation of V as follows.

First let V^* be the dual vector space of V. We need to define an action of G. Here, one important thing is taht for $g \in G$ and $f \in V^*$, we take

$$(g \cdot f)(v) := f(g^{-1}v)$$

for $v \in V$, using the inverse of g.

Theorem 77. *Let ψ_1, ψ_2 be characters of G. Then so is $\psi_1\psi_2$. In particular, $\mathcal{F}$ is closed under the product of class functions.*

More precisely, if $\psi_i = \mathrm{Tr}\,\varphi_i$ for representations φ_i, then $\psi_1\psi_2 = \mathrm{Tr}\,\varphi_1 \otimes \varphi_2$.

Theorem 78. *For a representation V of G, let χ be its character.*

Then the character for the dual representation V^* is the complex conjugate $\overline{\chi}$.

Corollary 11. *$\mathcal{F}$ is closed under sum, product and complex conjugation.*

Applications of Representation

Definition 45. Let G be a finite group. The *character table* of G means a table of the following form is

$$\begin{array}{c|cccc} & 1 = K_1 & K_2 & \cdots & K_r \\ & 1 = d_1 & d_2 & \cdots & d_r \\ \hline \chi_1 & 1 & 1 & \cdots & 1 \\ \chi_2 & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \chi_r & * & * & \cdots & * \end{array}$$

where $K_1, \cdots, K_r$ are the conjugacy classes, $d_1, \cdots, d_r$ are the sizes of the orbits, $\chi_1, \cdots, \chi_r$ are the irreducible characters.

The values are $\chi(g_j)$ where $g_j \in K_j$.

Theorem 79. *(1st Schur Orthogonality Theorem for Character Table)*

$$(\chi_i, \chi_j) = \frac{1}{|G|} \sum_{k=1}^r d_k \chi_i(g_k)\overline{\chi_j(g_k)} = \delta_{ij}$$

i.e. the weighted rows of the character table are orthogonal.

Theorem 80. *(2nd Schur Orthogonality Theorem for Character Table) For $x, y \in G$,*

$$\sum_{i=1}^{r} \chi_i(x)\overline{\chi_j(y)} = \begin{cases} |C_G(x)| & \text{if } x, y \text{ conjugate,} \\ 0 & \text{otherwise.} \end{cases}$$

i.e. the columns of the character table are orthogonal

Let $F(G, \mathbb{C}) = \mathrm{Mor}(G, \mathbb{C})$ be the set of all set-functions from G to $\mathbb{C}$.

Definition 46. For two functions $f_1, f_2 : G \to \mathbb{C}$, define the *convolution* to be a function $f_1 * f_2 : G \to \mathbb{C}$ given by

$$(f_1 * f_2)(g) = \sum_{h \in G} f_1(gh^{-1})f_2(h)$$

Corollary 12. *Consider the ring $(F(G, \mathbb{C}), +, *)$ with the coordinatewise sum and the convolution as the product. Then, the natural map $\mathbb{C}G \to (F(G, \mathbb{C}), +, *)$ is a ring isomorphism.*

Definition 47. Let $f \in F(G, \mathbb{C})$ and let $\varphi : G \to \mathrm{GL}(V)$ be a representation. Then the *Fourier transform of f at φ* is defined to be

$$\widehat{f}(\varphi) := \sum_{g \in G} f(g)\varphi(g)$$

Theorem 81. *(Peter-Weyl) For simple ring decomposition:*

$$\mathbb{C}G \simeq M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$$

, we can write it as

$$\mathbb{C}G \simeq \bigoplus_{i=1}^{r} \mathrm{End}(M_i)$$

Definition 48. Let F be a field, G be a group, $H \leq G$ be a subgroup. For a representation $\varphi : G \to \mathrm{GL}(M)$ of G, denote by $\mathrm{Res}_H^G M$ be the representation of H given by $H \to G \xrightarrow{\varphi} \mathrm{GL}(M)$. This is called the *restriction to H*.

Definition 49. Let F, G, H be as before. Let $\varphi : H \to \mathrm{GL}(L)$ be a representation. The induced representation $\mathrm{Ind}_H^G L$ is the representation of G given by $FG \otimes_{FH} L$. This is called the *induction to G*.

Theorem 82. Ind_H^G *and* Res_H^G *are adjoint functors.*

Theorem 83. *(Frobenius Reciprocity for Group Representation) Let M be a representation of H, N be a representation of G. Then we have a natural bijection*

$$\mathrm{Hom}_{FG}(\mathrm{Ind}_H^G M, N) \simeq \mathrm{Hom}_{FH}(M, \mathrm{Res}_H^G N)$$

This can be proved by the Adjunction Theorem.