MTH 302: Modules

Semester 2, 2013-2014

Dr. Prahlad Vaidyanathan

Contents

Finite Abelian Groups

(See [Norman, §1])

0.1. Fundamental Theorem of finite abelian groups

0.2. Examples :

(i) If $G = \langle g \rangle$ is cyclic, then $G \cong \mathbb{Z}/m\mathbb{Z}$ for some $m \in \mathbb{Z}$

(ii) If $G = \{g_1, g_2, \ldots, g_n\}$ finite abelian, then $G \cong \mathbb{Z}^n/K$ for some subgroup $K < \mathbb{Z}^n$

0.3. Definition :

(i) $\mathbb{Z}$-basis for $\mathbb{Z}^n$.

(ii) Notation : $K = \langle v_1, v_2, \ldots, v_t \rangle$

(iii) An invertible matrix $P \in M_n(\mathbb{Z})$

0.4. Examples :

(i) If $K = \langle (2,0), (0,4 \rangle$, then $G = \mathbb{Z}^2/K \cong \mathbb{Z}_2 \times \mathbb{Z}_4$

(ii) If $K' = \langle (4,6), (8,10) \rangle$, then write $A = \begin{pmatrix} 4 & 6 \\ 8 & 10 \end{pmatrix}$, then A is similar to $D = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$, and so $\mathbb{Z}^2/K' \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ as well.

0.5. Summary :

(i) Want to analyse a finite abelian group G, then write $G \cong \mathbb{Z}^n/K$ for some subgroup $K < \mathbb{Z}^n$

(ii) Find a $\mathbb{Z}$-basis $\{v_1, v_2, \ldots, v_t\}$ for K (Fact: Such a basis always exists with $t \leq n$)

(iii) Write $A = \begin{pmatrix} v_1 \\ v_2 \\ \cdots \\ v_t \end{pmatrix}$, then find invertible matrices P, T such that PAT^{-1} is diagonal (Fact: Such matrices P and T always exist)

(iv) Use the diagonal matrix to express G as a product of cyclic groups. The diagonal matrix is called the Smith Normal form of A.

(End of Day 1)

I. Rings

1. Definition and Examples

1.1. Definition of a ring

1.2. Examples :

(i) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. $\mathbb{N}$ is not a ring.

(ii) $2\mathbb{Z}$

(iii) $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

(iv) If R is a ring, then $M_n(R)$ is a ring

(v) $\mathbb{Z}[i]$

(vi) $C[0,1]$

(vii) If R is a ring, then $R[x]$ is a ring.

1.3. Definition :

(i) Multiplicative identity $1 = 1_R$. Note: If R has a multiplicative identity, then it is unique.

(ii) Commutative ring

(iii) Division ring

(iv) Field

(v) Zero divisor

(vi) Integral domain

1.4. Examples :

(i) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. $\mathbb{Z}$ is not.

(ii) $\mathbb{Z}_n$ is a field iff n is prime (See MTH 301.V.1.4)

(iii) $M_2(\mathbb{R})$ has zero divisors.

(iv) Any finite integral domain is a field.

(v) If R is an integral domain, then $R[x]$ is an integral domain.

1.5. Theorem: Let R be a ring, $a, b \in R$, then

(i) $0 \cdot a = a \cdot 0 = 0$

(ii) $(-a)b = a(-b) = -(ab)$

(iii) $(-a)(-b) = ab$

(iv) $(na)b = a(nb) = n(ab) \quad \forall n \in \mathbb{Z}$

1.6. Definition of subring.

1.7. Definition of ring homomomorphism, isomorphism.

1.8. Examples :

(i) The quotient map $\mathbb{Z} \to \mathbb{Z}_n$

(ii) $z \mapsto \overline{z}$ from $\mathbb{C}$ to $\mathbb{C}$

(iii) $f \mapsto f(0)$ from $C[0,1]$ to $\mathbb{C}$

(iv) $x \mapsto 2x$ from $\mathbb{Z}$ to $\mathbb{Z}$ is not a homomorphism.

1.9. Lemma: Let $\varphi : R \to R'$ be a ring homomorphism, then

(i) $\varphi(0_R) = O_{R'}$

(ii) $\varphi(-a) = -\varphi(a)$

1.10. Definition :

(i) Kernel of a homomorphism

(ii) Image of a homomorphism

1.11. Proposition : φ is injective iff $\ker(\varphi) = \{0\}$

2. Ideals and Quotient Rings

2.1. Definition of ideal

2.2. Examples :

(i) $n\mathbb{Z} \lhd \mathbb{Z}$

(ii) $\{f \in C[0,1] : f(0) = 0\} \lhd C[0,1]$

(iii) If $I \lhd R$, then $M_n(I) \lhd M_n(R)$. Proof that the converse is true in a commutative ring with 1.

(iv) If $\varphi : R \to R'$ is a homomorphism, then $\ker(\varphi) \lhd R$

(End of Day 2)

2.3. Theorem: Let R be a ring, and $I \lhd R$, then

$$R/I := \{a + I : a \in R\}$$

is a ring under the operations

$$(a + I) + (b + I) := (a + b) + I \text{ and } (a + I)(b + I) := (ab) + I$$

Furthermore, the function $\pi : R \to R/I$ given by

$$\pi(a) := a + I$$

is a surjective ring homomorphism and $\ker(\pi) = I$

2.4. (First Isomorphism Theorem): Let $\varphi : R \to R'$ be a ring homomorphism, then

(i) $\ker(\varphi) \lhd R$

(ii) $R/\ker(\varphi) \cong \mathrm{Im}(\varphi)$

In particular, if φ is surjective, then $R/\ker(\varphi) \cong R'$

2.5. Examples:

(i) If $R = C[0,1]$ and $I = \{f \in R : f(0) = 0\}$, then $R/I \cong \mathbb{C}$

(ii) If $I \lhd R$, then $M_n(R)/M_n(I) \cong M_n(R/I)$

(iii) If R is any ring, and $I = (x) := \{xf(x) : f(x) \in R[x]\} \lhd R[x]$, then $R[x]/I \cong R$.

2.6. (Correspondence theorem): If R is a ring, and $I \lhd R$, then there is a 1-1 correspondence between ideals in R/I and ideals in R containing I

2.7. Example : Ideals in $\mathbb{Z}_n \leftrightarrow \{$ divisors of $n\}$

2.8. Lemma : Let R be a ring. Let $\{S_\lambda : \lambda \in \Lambda\}$ be a (possibly uncountable) collection of ideals in R. Then

$$I := \bigcap_{\lambda \in \Lambda} S_\lambda$$

is an ideal in R

2.9. Definition : Let R be a ring, and $X \subset R$, then

$$(X) := \bigcap \{I \lhd R : X \subset I\}$$

is called the ideal generated by X. If $X = \{a\}$, we write $(a) = (\{a\})$, and we call (a) the *principal ideal* generated by a.

2.10. Lemma: Let R be a commutative ring with $1 \in R$, and let $X \subset R$, then

$$(X) = \bigcup_{k=1}^{\infty} \{\sum_{i=1}^{k} r_i x_i : r_i \in R, x_i \in X\}$$

ie. (X) consists of all finite sums of elements of the form rx where $r \in R, x \in X$. In particular,

$$(a) = \{ra : r \in R\}$$

2.11. Example : If $m, n \in \mathbb{Z}$, then $(\{m, n\}) = (gcd(m, n)) =: (m, n)$

(End of Day 3)

3. Prime and Maximal Ideals

Let R be a commutative ring with $1 \in R$

3.1. Definition of Maximal ideal

3.2. Theorem: R is a field iff R has no non-trivial ideals

3.3. Theorem: $I \lhd R$ is a maximal ideal iff R/I is a field

3.4. Examples:

(i) If $n \in \mathbb{Z}$ is prime iff $n\mathbb{Z} \lhd \mathbb{Z}$ is a maximal ideal.

(ii) $I := \{f \in C[0, 1] : f(0) = 0\} \lhd C[0, 1]$ is a maximal ideal.

(iii) $(x) \lhd F[x]$ is a maximal ideal if F is a field.

(iv) $(x) \lhd \mathbb{Z}[x]$ is not a maximal ideal.

3.5. Definition of prime ideal

3.6. Theorem: $I \lhd R$ is a prime ideal iff R/I is an integral domain.

3.7. Example : $n\mathbb{Z} \lhd \mathbb{Z}$ is prime iff n is a prime number.

3.8. Corollaries/Examples :

(i) $(x) \lhd \mathbb{Z}[x]$ is a prime ideal.

(ii) If $I \lhd R$ is a maximal ideal, then I is a prime ideal (3.3+3.7)

(iii) Let $\varphi : R \to R'$ be a surjective homomorphism, then $\ker(\varphi) \lhd R$ is prime (maximal) if R' is an integral domain (field)

4. The Chinese Remainder Theorem

Let R be a commutative ring with $1 \in R$

4.1. Definition :

(i) Sum of two ideals

(ii) Product of two ideals

(iii) Comaximal ideals

4.2. Lemma: Let $I, J \lhd R$ be comaximal ideals, then $IJ = I \cap J$

4.3. (Chinese Remainder Theorem): Let $I, J \lhd R$ and define

$$\varphi : R \to R/I \times R/J, \text{ given by } a \mapsto (a + I, a + J)$$

(i) φ is a homomorphism and $\ker(\varphi) = I \cap J$

(ii) If $I + J = R$, then φ is surjective, and $\ker(\varphi) = IJ$. In that case,

$$R/IJ \cong R/I \times R/J$$

(End of Day 4)

4.4. Corollary: If $I_1, I_2, \ldots, I_n \lhd R$ are such that for all $i \neq j$, one has $I_i + I_j = R$, then

$$R/(I_1 I_2 \ldots I_n) \cong R/I_1 \times R/I_2 \times \ldots \times R/I_n$$

4.5. Example :

(i) $m\mathbb{Z}, n\mathbb{Z} \lhd \mathbb{Z}$ are comaximal iff $(m, n) = 1$. In that case, $\mathbb{Z}_{nm} \cong \mathbb{Z}_m \times \mathbb{Z}_n$

(ii) In particular, if $n = p_1^{k_1} p_2^{k_2} \ldots p_t^{k_t}$, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_t^{k_t}}$$

4.6. Definition :

(i) Unit of a ring R

(ii) The group of units R^*

4.7. Lemma: $(R_1 \times R_2)^* \cong R_1^* \times R_2^*$

4.8. Corollary: If $n = p_1^{k_1} p_2^{k_2} \ldots p_t^{k_t}$, then

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{k_1}}^* \times \mathbb{Z}_{p_2^{k_2}}^* \times \ldots \times \mathbb{Z}_{p_t^{k_t}}^*$$

Hence

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1}) \ldots (p_t^{k_t} - p_t^{k_t - 1})$$

5. Unique Factorization Domains

Let R be an integral domain with $1 \in R$

5.1. Definition : Let $a, b \in R$

(i) $a \mid b$ (a divides b)

(ii) $a \sim b$ (a and b are associates)

5.2. Lemma :

(i) $a \mid b$ iff $(b) \subset (a)$

(ii) $a \sim b$ iff $(b) = (a)$. In particular, if u is a unit, then $(u) = R$

(iii) The relation $\sim$ is an equivalence relation.

5.3. Definition : Irreducible element

5.4. Remark :

(i) If $r, s \in R$ such that r is irreducible and $r \sim s$, then s is irreducible in R

(ii) Irreducibility depends on the ambient ring. $2 \in \mathbb{Z}$ is irreducible, but $2 \in \mathbb{Q}$ is a unit.

5.5. Definition : R is a UFD iff R satisfies

(UF1) Every element can be written as a product of irreducibles and units.

(UF2) The above decomposition is unique upto a change of order.

5.6. Examples :

(i) Every field is a UFD

(ii) $\mathbb{Z}$ is a UFD. In fact, every Euclidean domain is a UFD

(iii) $\mathbb{Z}[x]$ is a UFD (MTH 301: §$VI.4$)

(iv) $\mathbb{Z}[\sqrt{-5}]$ is not a UFD because $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ (with proof)

5.7. Definition : Prime element $p \in R$.

5.8. Lemma: Every prime is irreducible. Note: $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible, but not prime.

(End of Day 5)

5.9. Theorem: R is a UFD iff R satisfies **(UF1)** and

(UF2') Every irreducible is prime.

6. Principal Ideal Domains and Euclidean Domains

6.1. Definition

(i) Euclidean Domain

(ii) PID

6.2. Lemma: Every Euclidean domain is a PID

6.3. Examples :

(i) Every field is a Euclidean domain with $d \equiv 0$

(ii) $\mathbb{Z}$ is a Euclidean domain with $d(n) = |n|$

$\mathbb{Z}[i]$ is Euclidean domain with $d(a + bi) = a^2 + b^2$

(iii) If F is a field, $F[x]$ is a Euclidean domain with $d(f(x)) = deg(f(x))$

(iv) $\mathbb{Z}[x]$ is not a PID (See MTH 301, Example § VI.4.3)

(v) If $\omega = (1 + \sqrt{-19})/2$, then $\mathbb{Z}[w]$ is a PID, but not a Euclidean domain (proof omitted)

6.4. Lemma: Every PID satisfies **(UF1)**

(End of Day 6)

6.5. Definition: Greatest Common Divisor (GCD)

6.6. Lemma: Let R be a PID, and $a, b \in R$. Then

(i) (a, b) exists in R

(ii) $\exists x, y \in R$ such that $(a, b) = ax + by$

6.7. Theorem: Every PID is a UFD.

II. Modules

1. Definition and Examples

Let R be a commutative ring with $1 \in R$

1.1. Definition of module M over R

1.2. Examples :

(i) R as a module over itself

(ii) A vector space over a field k is a k-module.

(iii) An abelian group is a $\mathbb{Z}$-module. In fact, every $\mathbb{Z}$-module is nothing but an abelian group.

(iv) A linear transformation $T : V \to V$ gives V the structure of a $k[x]$-module via $f(x) \cdot v := f(T)(v)$. In fact, a $k[x]$-module is nothing but a vector space with a specific linear transformation $T : V \to V$.

1.3. Lemma: Let M be an R-module, then for all $r \in R, m \in M$,

(i) $0_R \cdot m = 0_M$

(ii) $r \cdot 0_M = 0_M$

(iii) $(-r) \cdot m = -(r \cdot m) = r \cdot (-m)$

1.4. Definition of submodule $N < M$

1.5. Examples :

(i) If R is thought of as a module over R, then any submodule is an ideal $I \lhd R$

(ii) If V is a vector space over k, then any subspace $W < V$ is a k-submodule.

(iii) If G is an abelian group, any subgroup $H < G$ is a $\mathbb{Z}$-submodule.

(iv) If $T : V \to V$ is a linear transformation making V into a $k[x]$-module, then a $k[x]$-submodule is a vector subspace $W \subset V$ such that $T(W) \subset W$.

(End of Day 7)

2. Homomorphisms and Quotient Modules

2.1. Definition

(i) Module homomorphism $\theta : M \to M'$

(ii) Isomorphism of modules (In this case, we write $M \cong M'$)

2.2. Examples :

(i) The zero map

(ii) If G, G' are $\mathbb{Z}$-modules (abelian groups), then module homomorphism $\leftrightarrow$ group homomorphism

(iii) If V, W are k-modules (vector spaces), then module homomorphism $\leftrightarrow$ linear transformation

(iv) If R is a ring thought of as an R-module, then a module homomorphism is not the same as a ring homomorphism. For instance $x \mapsto 2x$ from $\mathbb{Z}$ to $\mathbb{Z}$ is a module homomorphism, but not a ring homomorphism.

(v) If (V, A) and (W, B) are $k[x]$-modules (as in Example 1.2.(iv)), then a module homomorphism is a linear map $T : V \to W$ such that $TA = BT$. In particular, $(V, A) \cong (W, B)$ iff A and B are similar.

2.3. Definition: $\theta : M \to M'$ a homomorphism of R-modules

(i) $\ker(\theta) < M$

(ii) $\mathrm{Im}(\theta) < M'$

2.4. Lemma: θ is injective iff $\ker(\theta) = \{0_M\}$

2.5. Theorem: If $N < M$, then M/N is an R-module via the map $(r, a + N) \mapsto ra + N$

2.6. (First Isomorphism theorem): Let $\theta : M \to M'$ be a homomorphism of R-modules, then

$$M/\ker(\theta) \cong \mathrm{Im}(\theta)$$

In particular, if θ is surjective, then $M/\ker(\theta) \cong M'$

2.7. (Second Isomorphism theorem): Let M be an R-module, and $L, K < M$, then

(i) $L + K = \{l + k : l \in L, k \in K\} < M$

(ii) $L/L \cap K \cong (L + K)/K$

2.8. (Third Isomorphism theorem): Let M be an R-module and $L, K < M$ such that $K \subset L$, then

$$(M/K)/(L/K) \cong M/L$$

2.9. (Correspondence theorem): Let M be an R-module, and $N < M$, then there is a one-to-one correspondence between the set of submodules of M/N and the submodules of M that contain N

(End of Day 8)

3. Direct Sums of Modules

3.1. Definition

(i) External Direct Sum

Notation: $R^n = \oplus_{i=1}^n R$

(ii) Internal Direct Sum

3.2. Theorem : If $M_1, M_2, \ldots, M_n < M$, then M is the internal direct sum of $M_1, M_2, \ldots M_n$ iff

(i) $M = M_1 + M_2 + \ldots + M_n$

(ii) For each $1 \leq i \leq n$, $M_i \cap \sum_{j \neq i} M_j = \{0\}$

3.3. Theorem: If M is the internal direct sum of $M_1, M_2, \ldots, M_n$, then

$$M \cong M_1 \oplus M_2 \oplus \ldots \oplus M_n$$

3.4. Definition: Suppose M is the internal direct sum of $M_1, M_2, \ldots, M_n$

(i) Components of $m \in M$

(ii) Projection map $\pi_i : M \to M_i \subset M$

3.5. Remark: Suppose M is the internal direct sum of $M_1, M_2, \ldots, M_n$, then

(i) $M_i = \mathrm{Im}(\pi_i)$

(ii) $\pi_i^2 := \pi_i \circ \pi_i = \pi_i$

(iii) $\sum_{i=1}^n \pi_i = \mathrm{id}_M$

4. Finitely Generated Modules

4.1. Lemma: Let $\{N_\lambda\}_{\lambda \in \Lambda}$ be a collection of R-submodules of M, then $\bigcap_{\lambda \in \Lambda} N_\lambda$ is an R-submodule.

4.2. Definition of a submodule $\langle X \rangle$ generated by a set X

Note: By Lemma 4.1, $\langle X \rangle < M$

4.3. Lemma: Let M be an R-module and $X \subset M$ any set, then

$$\langle X \rangle = \bigcup_{k=1}^{\infty} \{ \sum_{i=1}^{k} r_i n_i : r_i \in R, n_i \in N \}$$

4.4. Definition:

(i) Finitely generated (f.g.) module

(ii) Cyclic module

4.5. Examples :

(i) (a) R is a cyclic module over R with generator 1

(b) If $I \lhd R$, then I is cyclic iff I is principal (There is no special name for a f.g. ideal)

(c) $R/I = \langle 1 + I \rangle$ is cyclic.

(ii) (a) A k-vector space V is a finitely generated k-module iff it is finite dimensional.

(b) It is cyclic iff $\dim(V) \in \{0, 1\}$

(c) c_0 is an infinite dimensional vector space.

(End of Day 9)

(iii) A cyclic $\mathbb{Z}$-module is a cyclic abelian group. Any finite abelian group is a finitely generated $\mathbb{Z}$-module. $\mathbb{Z}$ is a finitely generated $\mathbb{Z}$-module. Hence,

$$\mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z} \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$$

is a finitely generated $\mathbb{Z}$-module. We will show that all finitely generated abelian groups look like this.

(iv) $R^n \oplus R/I_1 \oplus R/I_2 \oplus \ldots \oplus R/I_k$ is a f.g. R-module We will show that, if R is a PID, then all f.g. R-modules look like this

(v) In particular, if (V, T) is the f.g. $k[x]$-module from Example 2.2.(v), then

$$(V, T) \cong k[x]^n \oplus k[x]/(g_1(x)) \oplus k[x]/(g_2(x)) \oplus \ldots \oplus k[x]/(g_k(x))$$

for some ideals $I_1, I_2, \ldots, I_n \lhd k[x]$. This allows us to determine when two linear operators are similar.

(vi) A submodule of a f.g. module may not be f.g. : Let $R = C_b(\mathbb{R})$ be the ring of continuous, bounded functions $f : \mathbb{R} \to \mathbb{R}$, and consider R as a module over itself. Let

$$I = C_c(\mathbb{R}) = \{ f \in R : \exists M > 0 \text{ such that } f(x) = 0 \quad \forall |x| \geq M \}$$

Then $I < R$, but I is not f.g., even though R is f.g. (in fact, cyclic)

4.6. Definition : Rank $\mu(M)$ of a module M. If M is not f.g, then $\mu(M) = +\infty$

4.7. Proposition: Let M be an R-module and $N < M$.

(i) It may happen that $\mu(M) < \infty$, $N < M$, but $\mu(N) = +\infty$

(ii) If $N < M$, then $\mu(M/N) \leq \mu(M)$

(iii) Suppose N and M/N are f.g., then so if M and $\mu(M) \leq \mu(N) + \mu(M/N)$

4.8. Definition : Let M be an R-module

(i) Linearly dependent set $\{x_1, x_2, \ldots, x_n\} \subset M$

(ii) Linearly independent set

(iii) Torsion-free element

Note: Every non-zero element of a vector space is torsion-free. However, no element of $\mathbb{Z}_n$ is torsion-free (when $\mathbb{Z}_n$ is thought of as $\mathbb{Z}$-module)

4.9. Theorem : Let M be an R-module and $X := \{x_1, x_2, \ldots, x_n\} \subset M$ be a finite set. Then, TFAE :

(i) X is linearly independent and $M = \langle X \rangle$

(ii) For every $m \in M, \exists! r_i \in R$ such that $m = \sum r_i x_i$

(iii) Each x_i is torsion-free and $M \cong \langle x_1 \rangle \oplus \langle x_2 \rangle \oplus \ldots \oplus \langle x_n \rangle$

(End of Day 10)

4.10. Definition :

(i) X generates M freely

(ii) Basis

4.11. Examples:

(i) $R = \langle 1 \rangle$ and R^n are freely generated R-modules.

(ii) Any f.g. k-vector space is freely generated by its basis.

(iii) $\mathbb{Z}_n$ is free as a $\mathbb{Z}_n$-module, but not as a $\mathbb{Z}$-module

(iv) Let (V, T) be a $k[x]$-module as in Example 1.2.(iv), then (V, T) is not a free module since every $v \in V$ has torsion.

(v) Every generating set of a vector space contains a basis. However, $\{2, 3\} \subset \mathbb{Z}$ generates $\mathbb{Z}$ as a $\mathbb{Z}$-module, but it does not contain a basis.

4.12. Definition :

(i) Annihilator $Ann(m)$. Note: $Ann(m) \lhd R$

(ii) Torsion module/Torsion-free module

(iii) M_τ is the torsion submodule

4.13. Examples:

(i) A k-vector space is torsion-free as a k-module

(ii) If R is an integral domain, then every non-zero element of R (as a module over itself) is torsion-free

(iii) (V, T) is a torsion $k[x]$-module

(iv) For an Abelian group G, G_τ is the set of elements of finite order. $\mathbb{Z}^n, \mathbb{Q}$ are torsion-free, and $G = \mathbb{Z}_n$ are torsion $\mathbb{Z}$-modules; and $\mathbb{Z} \oplus \mathbb{Z}_2$ is neither torsion nor torsion-free.

4.14. Proposition: Let R be an integral domain, and M an R-module. Then

(i) $M_\tau < M$

(ii) M/M_τ is torsion-free

III. Finitely Generated Modules over a PID

Let R be a PID, and M a f.g. module over R

1. Free Modules over a PID

1.1. Definition: Free-rank of M, $f(M)$

Note: $\mu(M) \leq f(M)$, but they may not be equal. Will show that they are equal when R is a PID.

(End of Day 11)

1.2. Theorem: Let R be a PID, and M a f.g., free R-module. If $N < M$, then N is a free R-module and $f(N) \leq f(M)$

1.3. Lemma: Let M be a f.g. R-module, then $\exists$ a free R-module F such that $f(F) = \mu(M)$ and $M \cong F/N$ for some submodule $N < F$

1.4. Corollary: Let M be a f.g. module over a PID R and $N < M$, then N is f.g. and $\mu(N) \leq \mu(M)$

1.5. Lemma: If M is free, then M is torsion-free. (Proof as HW)

1.6. Theorem: A finitely generated torsion-free module is free, and $f(M) = \mu(M)$

(End of Day 12)

1.7. Theorem: Let M be a free R-module, then

(i) $\exists n \in \mathbb{N} \cup \{0\}$ such that $M \cong R^n$

(ii) $R^n \cong R^m$ iff $n = m$

1.8. Lemma: If $\theta : M \to F$ is a surjective map where M is f.g. and F is free, then $M \cong F \oplus \ker(\theta)$

1.9. Theorem: Let M be a f.g. module over R. Then

(i) M/M_τ is free

(ii) $\exists n \in \mathbb{N} \cup \{0\}$ such that $M \cong R^n \oplus M_\tau$

Moreover, n is uniquely determined by M and is called the rank of M.

1.10. Remark:

(i) If $n = \mu(M/M_\tau)$, then any set of $(n+1)$ elements of M is linearly dependent.

(ii) Let M, N be two f.g. R-modules, then $M \cong N$ iff

$$M_\tau \cong N_\tau \text{ and } \operatorname{rank}(M) = \operatorname{rank}(N)$$

(iii) A torsion module is nothing but a module of rank 0. It now suffices to classify torsion modules.

2. Torsion Modules over a PID - I

(See [Lang, §III.7]) Let M be a f.g. torsion module over a PID R

2.1. Definition:

(i) For $x \in M$, recall that

$$\operatorname{Ann}(x) := \{a \in R : ax = 0\} \lhd R$$

Hence, $\exists d \in R$ such that $\operatorname{Ann}(x) = (d)$. This d is unique upto multiplication by a unit (by Lemma I.5.2), and is called the *order* of x, denoted by $O(x)$

(ii) Recall that

$$\operatorname{Ann}(M) := \{a \in R : ax = 0 \quad \forall x \in M\} \lhd R$$

By HW 3.3, $\operatorname{Ann}(M) \neq \{0\}$, and so $\exists a \in R$ such that $\operatorname{Ann}(M) = (a)$. This a is unique upto multiplication by a unit and is called the *exponent* of M

(iii) Let $p \in R$ prime, then the *p-primary component* of M is

$$M(p) := \{x \in M : p^n x = 0 \text{ for some } n \in \mathbb{N}\}$$

(End of Day 13)

2.2. Examples :

(i) If G is an abelian group, the order of $x \in G$ as a $\mathbb{Z}$-module is the same as the order of $x \in G$ as an abelian group.

(ii) If G is an abelian group, the exponent of G may not be the order of G. For instance, the exponent of $\mathbb{Z}_p \oplus \mathbb{Z}_p$ is p, but its order is p^2

(iii) If G is a finite abelian group, the p-primary component of G is merely the p-Sylow subgroup of G

(iv) If $M = (V, T)$ is the $k[x]$-module, then the exponent of M is the minimal polynomial of T

2.3. Lemma: Let M be a f.g. torsion R-module, with exponent a. Since R is a PID, it is a UFD (by Theorem I.6.7). Write

$$a = up_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

as where $u \in R^*$ and $p_1, p_2, \dots, p_k$ are prime elements of R. Then

$$M = M(p_1) \oplus M(p_2) \oplus \dots \oplus M(p_k)$$

2.4. Remark: Suppose M is a f.g. torsion R-module such that $M = M(p)$ for some prime $p \in R$. Write $M = \langle x_1, x_2, \dots, x_n \rangle$, then $\exists \beta_i \in \mathbb{N}$ such that $p^{\beta_i} x_i = 0$ for all i. Then, for $\beta = \max\{\beta_i : 1 \le i \le n\}$, we have

(i) p^β is the exponent of M

(ii) $\exists z \in M$ such that $O(z) = p^\beta$. We say that z has maximal order in M

2.5. Lemma: Let M be a f.g. torsion R-module such that $M = M(p)$, and $z \in M$ have maximal order. Write $N = \langle z \rangle$, then for any $x + N \in M/N, \exists y \in M$ such that $O(x) = O(y)$

2.6. Theorem: Let M be a f.g. torsion R-module such that $M = M(p)$, then $\exists$ natural numbers $\alpha_1 \ge \alpha_2 \ge \dots \ge \alpha_k \ge 1$ such that

$$M \cong R/(p^{\alpha_1}) \oplus R/(p^{\alpha_2}) \oplus \dots \oplus R/(p^{\alpha_k})$$

(End of Day 14)

2.7. Corollary: Let M be a f.g. torsion module over a PID R, then $\exists$ prime elements $p_1, p_2, \dots p_k \in R$, and integers $\{\alpha_{i,j} : 1 \le i \le k, 1 \le j \le \nu_i\}$ such that

$$M \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{\nu_i} R/(p_i^{\alpha_{i,j}})$$

The list

$$\begin{gathered}\{p_1^{\alpha_{1,1}}, p_1^{\alpha_{1,2}}, \dots, p_1^{\alpha_{1,\nu_1}}, \\ p_2^{\alpha_{2,1}}, p_2^{\alpha_{2,2}}, \dots, p_2^{\alpha_{2,\nu_2}}, \\ \vdots \quad \vdots \qquad \vdots \\ p_k^{\alpha_{k,1}}, p_k^{\alpha_{k,2}}, \dots, p_k^{\alpha_{k,\nu_k}}\}\end{gathered}$$

is called the list of *elementary divisors of* M, denoted by $El(M)$

2.8. Corollary: Let M be a f.g. torsion R-module, then $\exists d_1, d_2, \dots, d_n \in R$ such that

$$d_1 \mid d_2 \mid \dots \mid d_t$$

and

$$M \cong R/(d_1) \oplus R/(d_2) \oplus \dots \oplus R/(d_t)$$

The list

$$\{d_1, d_2, \dots, d_t\}$$

is called the list of *invariant factors of* M

3. Torsion Modules over a PID - II

(See [Hartley, §9.2])

3.1. Lemma: For $p \in R$ a prime element, and $\alpha \geq 1$, let $L = R/(p^\alpha)$. If $\varphi, \psi : L \to L$ be homomorphisms such that

$$\varphi + \psi = \mathrm{id}_L$$

then, either φ or ψ is bijective.

(End of Day 15)

3.2. Lemma: If $M = M_1 \oplus M_2$, and $N < M$ containing M_1, then $N = M_1 \oplus (N \cap M_2)$

3.3. (Cancellation Lemma): Let T be a f.g. torsion R-module, and N_1, N_2 two R-modules, then

$$T \oplus N_1 \cong T \oplus N_2 \Rightarrow N_1 \cong N_2$$

3.4. (Uniqueness of Invariant Factor decomposition): Suppose $d_1, d_2, \ldots, d_t \in R$ and $d'_1, d'_2, \ldots, d'_s \in R$ such that

$$d_1 \mid d_2 \mid \ldots \mid d_t \text{ and } d'_1 \mid d'_2 \mid \ldots \mid d'_s$$

and

$$R/(d_1) \oplus R/(d_2) \oplus \ldots \oplus R/(d_t) \cong R/(d'_1) \oplus R/(d'_2) \oplus \ldots R/(d'_s)$$

then $s = t$, and $d_i \sim d'_i$ for all $1 \leq i \leq t$.

3.5. Remark: The list of invariant factors is uniquely determined by M, and hence so is the list of elementary divisors.

3.6. (Structure Theorem for Modules over PIDs) : Let M be a finitely generated module over a PID R

(i) There exists $n \in \mathbb{N} \cup \{0\}$, prime elements $p_1, p_2, \ldots p_k \in R$, and integers $\{\alpha_{i,j} : 1 \leq i \leq k, 1 \leq j \leq \nu_i\}$ such that $1 \leq \alpha_{i1} \leq \alpha_{i2} \leq \ldots \leq \alpha_{i\nu_i}$ and

$$M \cong R^n \left[\bigoplus_{i=1}^{k} \oplus_{j=1}^{\nu_i} R/(p_i^{\alpha_{i,j}}) \right]$$

(ii) If N is another finitely generated modules over a PID R, then

$$M \cong N \Leftrightarrow \begin{cases} \text{Elementary Divisors of } M = \text{Elementary divisors of } N, \text{ and} \\ rank(M) = rank(N) \end{cases}$$

(End of Day 16)

4. Finite Abelian Groups

4.1. (Structure theorem for finite abelian groups): Let G be a finite abelian group

(i) There exist prime numbers $p_1, p_2, \ldots p_k \in \mathbb{Z}$, and integers $\{\alpha_{i,j} : 1 \leq i \leq k, 1 \leq j \leq \nu_i\}$ such that $1 \leq \alpha_{i1} \leq \alpha_{i2} \leq \ldots \leq \alpha_{i\nu_i}$ and

$$G \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{\nu_i} \mathbb{Z}_{p_i^{\alpha_{i,j}}}$$

(ii) If G' is another finite abelian group, then

$$G \cong G' \Leftrightarrow El(G) = El(G')$$

4.2. Corollary: The number of non-isomorphic abelian groups of order p^n, where $p \in \mathbb{Z}$ is a prime is equal to $\pi(n)$, the number of partitions of n.

Example: $p = 5, n = 4$

4.3. Corollary: Let $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$, then the number of non-isomorphic abelian groups of order n is equal to $\pi(k_1)\pi(k_2)\ldots\pi(k_n)$

Example: Abelian groups of order 600.

4.4. Theorem: Let G be a finite abelian group, and $m \mid |G|$, then $\exists H < G$ such that $|H| = m$ (Proof as HW)

Example: If $G = \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3$, then $|G| = 864$. $144 \mid |G|$, so $\exists H < G$ such that $|H| = 144$. We may take $H = \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \{0\} < G$

4.5. Theorem: Let F be a field, and $G \subset F^* = F \setminus \{0\}$ be a finite subgroup of the multiplicative group F^*. Then, G is a cyclic group. In particular, $\mathbb{Z}_p^*$ is a cyclic for all primes p

4.6. Example: Let $n = p_1 p_2 \ldots p_k$ be square-free, then

(i) There is exactly one abelian group of order n, viz. $\mathbb{Z}_n$

(ii) $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1-1} \times \mathbb{Z}_{p_2-1} \times \ldots \times \mathbb{Z}_{p_k-1}$

(iii) In particular, if n is divisible by two distinct odd primes, then $\mathbb{Z}_n^*$ is not cyclic. In fact, $\mathbb{Z}_n^*$ is cyclic iff $n \in \{2, 4, p^k, 2p^k\}$ for some odd prime p (without proof)

5. Rational Canonical Form

(See [Adkins, §4.4])

Let V be a finite dimensional vector space over a field k. Let $T : V \to V$ be a linear transformation. Consider $M = (V, T)$ as a $k[x]$-module as in Example II.1.2

5.1. Remark :

(i) By Example II.1.5, There is a 1-1 correspondence between submodules of M and subspaces of V that are T-invariant.

(ii) By Example II.2.2, There is a 1-1 correspondence between $k[x]$-module homomorphisms $\varphi : (V,T) \to (W,T')$ and linear maps $S : V \to W$ such that $ST = T'S$

(iii) $(V,T) \cong (V,T')$ iff T and T' are similar.

(iv) By Example II.4.11, M is a f.g. torsion $k[x]$-module.

(v) Hence, by Theorem III.3.6, there exist polynomials $f_1(x), f_2(x), \ldots, f_k(x) \in k[x]$ such that $f_1(x) \mid f_2(x) \mid \ldots \mid f_k(x)$ and

$$M \cong k[x]/(f_1(x)) \oplus k[x]/(f_2(x)) \oplus \ldots \oplus k[x]/(f_k(x))$$

These $f_i(x)$ are unique upto multiplication by a unit. Since $k[x]^* = k^*$, we may choose the $f_i(x)$ to be monic polynomials, in which case they are simply unique. The set $\{f_1(x), f_2(x), \ldots, f_k(x)\}$ so chosen is called the list of *invariant factors* of T

(vi) We define the characteristic polynomial of T to be $c_T(x) := f_1(x)f_2(x)\ldots f_k(x)$

(vii) We define the minimal polynomial of T to be the unique monic polynomial $m_T(x) \in k[x]$ such that $\mathrm{Ann}(M) = \langle m_T(x) \rangle$. Note: $m_T(x) = f_k(x)$ and $m_T(x) \mid c_T(x)$

(End of Day 17)

Notation: Let $\mathcal{B}$ be a basis for V, then $[T]_{\mathcal{B}}$ denotes the matrix of T w.r.t. $\mathcal{B}$

5.2. Lemma: Let $T : V \to V$ be a linear transformation, and suppose $V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$, where each V_i is T-invariant. Let $\mathcal{B}_i$ be a basis for V_i, then $\mathcal{B} = \cup \mathcal{B}_i$ is a basis for V, and

$$[T]_{\mathcal{B}} = \begin{bmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & & \vdots \\ \vdots & & & 0 \\ 0 & \ldots & & A_k \end{bmatrix}$$

where $A_i = [T\mid_{V_i}]_{\mathcal{B}_i}$.

Conversely, if the matrix of T w.r.t some basis $\mathcal{B}$ of V has the above form, then V splits up as the direct sum of T-invariant subspaces as above.

Notation:

(i) $T = T_1 \oplus T_2 \oplus \ldots \oplus T_k$, where $T : V \to V$ is a linear transformation

(ii) $A = A_1 \oplus A_2 \oplus \ldots \oplus A_k$, where $A \in M_n(k)$ is a matrix

5.3. Definition: A linear transformation $T : V \to V$ is called *cyclic of order* $f(x)$ iff (V,T) is a cyclic $k[x]$-module, and $\exp(V,T) = f(x)$

5.4. Lemma: Suppose T is cyclic of order $f(x)$, write

$$f(x) = a_0 + a_1 x + \ldots + a_{m-1}x^{m-1} + x^m$$

then

(i) $\exists 0 \neq v \in V$ such that $\{v, T(v), T^2(v), \ldots, T^{m-1}(v)\}$ is a basis for V. In particular, $\dim(V) = \deg(f(x))$

(ii) The matrix of T w.r.t $\mathcal{B}$ is given by

$$[T]_{\mathcal{B}} = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ \vdots & \vdots & & & & \vdots \\ 0 & 0 & \ldots & 1 & 0 & -a_{m-2} \\ 0 & 0 & \ldots & 0 & 1 & -a_{m-1} \end{bmatrix}$$

5.5. Definition: Companion matrix $C(f)$ for a polynomial $f(x) \in k[x]$

5.6. Examples:

(i) $C(x - \lambda) = [\lambda] \in M_1(k)$

(ii) $\text{diag}(a_1, a_2, \ldots, a_n) = \bigoplus_{i=1}^{n} C(X - a_i)$

(iii) $C(X^2 + 1) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

(iv) If $A = C(X - a) \oplus C(X^2 - 1)$, then

$$A = \begin{bmatrix} a & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

5.7. Theorem: Let $T : V \to V$, then V has a basis $\mathcal{B}$ such that

$$[T]_{\mathcal{B}} = C(f_1) \oplus C(f_2) \oplus \ldots \oplus C(f_k)$$

where $\{f_1(x), f_2(x), \ldots, f_k(x)\}$ are the invariant factors of T.

(End of Day 18)

5.8. Definition :

(i) Let $T : V \to V$ be a linear transformation, then the matrix described in Theorem 5.9 is called the *rational canonical matrix* of T

(ii) If $A \in M_n(k)$ is any matrix, then define $T : k^n \to k^n$ by $T(v) = Av$, then the corresponding matrix for T is called the *rational canonical form (RCF)* of A.

Note: Any matrix $A \in M_n(k)$ is similar to its rational canonical form, and that any two matrices $A, B \in M_n(k)$ are similar iff they have the same rational canonical form.

5.9. Example: Conjugacy classes in $GL_2(\mathbb{Z}_p)$

(i) For $A \in GL_2(\mathbb{Z}_p)$, write $k = \mathbb{Z}_p, V = \mathbb{Z}_p^2$ and $T_A : V \to V$ given by $v \mapsto Av$. Let $M = (V, T_A)$, then

$$M \cong k[x]/(f_1(x)) \oplus k[x]/(f_2(x)) \oplus \ldots \oplus k[x]/(f_k(x))$$

Since $\dim(V) = 2$, it follows that $k \leq 2$

(ii) If $k = 2$, then the RCF of A must belong to

$$C_1 = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{Z}_p^* \right\},$$

(iii) If $k = 1$, and $f_1(x)$ is irreducible, then the RCF of A must belong to

$$C_2 = \left\{ \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} : a_0 + a_1 x + x^2 \in \mathbb{Z}_p[x] \text{ irreducible} \right\}$$

(iv) If $k = 1$ and $f_1(x)$ is composite with two distinct roots, then the RCF of A must belong to

$$C_3 = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} : \lambda, \mu \in \mathbb{Z}_p^*, \lambda \neq \mu \right\}$$

(v) If $k = 1$ and $f_1(x)$ is composite with the same repeated root, then the RCF of A must belong to

$$C_4 = \left\{ \begin{pmatrix} 0 & -\lambda^2 \\ 1 & 2\lambda \end{pmatrix} : \lambda \in \mathbb{Z}_p^* \right\}$$

(vi) Hence, the representatives for the conjugacy classes in $GL_2(\mathbb{Z}_p)$ are

$$C_1 \cup C_2 \cup C_3 \cup C_4$$

and so the number of conjugacy classes is $(p^2 - 1)$ (HW)

(End of Day 19)

6. Cayley-Hamilton Theorem

6.1. Definition:

(i) Characteristic polynomial $c_T(x)$ for $T : V \to V$

(ii) Characteristic polynomial $c_A(x)$ for $A \in M_n(k)$

6.2. Lemma: Let $f(x) \in k[x]$ be a monic polynomial, and $A = C(f)$ be its companion matrix, then

$$\det(xI - A) = f(x)$$

6.3. Lemma: Let $A, B \in M_n(k)$ be similar matrices, then $c_A(x) = c_B(x)$. In particular, if (V, T) as before, and $\mathcal{B}$ and $\mathcal{B}'$ are two different bases for V, then

$$c_{[T]_{\mathcal{B}}}(x) = c_{[T]_{\mathcal{B}'}}(x)$$

6.4. Proposition: Let $T : V \to V$ be a linear transformation on a finite dimensional k-vector space as before, then for any basis $\mathcal{B}$ of V, we have

$$c_T(x) = c_{[T]_{\mathcal{B}}}(x)$$

6.5. (Cayley-Hamilton Theorem): Let $T : V \to V$ be a linear transformation on a finite dimensional vector space V, and let $\mathcal{B}$ be any basis for V. If $A = [T]_{\mathcal{B}}$, then

$$c_A(T) = 0$$

6.6. Remark: Cayley-Hamilton theorem is usually phrased as *A linear transformation satisfies its own characteristic polynomial.* Here, the fact that $c_T(T) = 0$ is trivial (since $m_T(x) \mid c_T(x)$), but the fact that $c_A(T) = 0$ is non-trivial.

7. Jordan Canonical Form

Note: If $T(x) = \lambda x$ for all $x \in V$, then

(i) $m_T(x) = (x - \lambda)$ and $c_T(x) = (x - \lambda)^n$

(ii) The rational canonical matrix of T is not a diagonal matrix, and hence not very useful.

In this section, we assume that $k = \mathbb{C}$

7.1. (Fundamental Theorem of Algebra): The primes in $\mathbb{C}[x]$ are of the form $(x - \lambda)$ for some $\lambda \in \mathbb{C}$ (without proof)

7.2. Remark: Let $M = (V, T)$ be a $\mathbb{C}[x]$-module as before. The elementary divisor decomposition of M in Theorem III.2.7 is of the form

$$M \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{\nu_i} \mathbb{C}[x]/(x - \lambda_i)^{n_{ij}}$$

where $\{\lambda_1, \lambda_2, \ldots, \lambda_k\}$ are distinct complex numbers, and, for each $1 \leq i \leq k$, one has $1 \leq n_{i1} \leq n_{i2} \leq \ldots \leq n_{i\nu_i}$. Consider the subspaces

$$V_{i,j} \leftrightarrow \mathbb{C}[x]/(x - \lambda_i)^{n_{ij}}$$

Note that $T(V_{ij}) \subset V_{ij}$. As in Section III.5, we will find a basis $\mathcal{B}_{i,j}$ of $V_{i,j}$ such that

$$A_{i,j} := [T \mid_{V_{i,j}}]_{\mathcal{B}_{i,j}}$$

is in a *nice* form. Then, with $\mathcal{B} = \cup_{i,j} \mathcal{B}_{i,j}$, by Lemma III.5.2, $\mathcal{B}$ is a basis for V, and

$$[T]_{\mathcal{B}} = \bigoplus_{i,j} A_{i,j}$$

7.3. Definition: For $\lambda \in \mathbb{C}$, the $n \times n$ Jordan block with value λ is denoted by $J_{\lambda,n}$

(End of Day 20)

7.4. Lemma:

(i) For $1 \leq k \leq (n-1)$, $(J_{\lambda,n} - \lambda I_n)^k \neq 0$, but

$$(J_{\lambda,n} - \lambda I_n)^n = 0$$

(ii) If $V = \mathbb{C}^n$ and $T : V \to V$ is given by $v \mapsto J_{\lambda,n}v$, then

$$m_T(x) = (x - \lambda)^n = c_T(x)$$

(iii) $M = (V, T)$ is a cyclic $\mathbb{C}[x]$-module

7.5. Proposition: Let (V, T) be as before, and suppose $M = (V, T)$ is a cyclic $\mathbb{C}[x]$-module with

$$m_T(x) = (x - \lambda)^n$$

for some $\lambda \in \mathbb{C}$ and $n \in \mathbb{N}$. Then,

(i) $\exists 0 \neq v \in V$ such that

$$\mathcal{B} = \{v, (T - \lambda)(v), (T - \lambda)^2(v), \ldots, (T - \lambda)^{n-1}(v)\}$$

forms a basis for V

(ii) $[T]_{\mathcal{B}} = J_{\lambda,n}$

7.6. Theorem: Let V be a finite dimensional complex vector space and $T : V \to V$ be a linear operator. Then $\exists$ a basis $\mathcal{B}$ of V such that

$$[T]_{\mathcal{B}} = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{\nu_i} J_{\lambda_i, n_{i,j}}$$

where $\{\lambda_1, \lambda_2, \ldots, \lambda_k\}$ are distinct complex numbers and, for each $\leq i \leq k$, $1 \leq n_{i1} \leq n_{i2} \leq \ldots \leq n_{i\nu_i}$.

7.7. Remark: Theorem 7.6 is true over any field k, provided all the irreducible factors of $m_T(x)$ are linear (See HW 5.6)

7.8. Definition:

(i) Jordan Canonical matrix of a transformation $T : V \to V$

(ii) Jordan canonical form of a matrix $A \in M_n(\mathbb{C})$.

Note: Two matrices have the same Jordan Canonical form iff they are similar.

(iii) Generalized Eigen-value, Generalized Eigen-vector

(iv) Generalized Eigen-space = $(x - \lambda)$-primary component

7.9. Example: Let $T : \mathbb{C}^2 \to \mathbb{C}^2$ be a linear transformation, and let $c_T(x) = (x - \lambda_1)(x - \lambda_2)$, then the JCF of T is one of

(i) If $\lambda_1 \neq \lambda_2$: $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$

(ii) If $\lambda_1 = \lambda_2$:

(a) If $m_T(x) = (x - \lambda_1)$: $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1 \end{pmatrix}$

(b) If $m_T(x) = (x - \lambda_1)^2$: $\begin{pmatrix} \lambda_1 & 1 \\ 0 & \lambda_1 \end{pmatrix}$

(End of Day 21)

IV. Introduction to Commutative Algebra

1. Hom and Direct Sums

1.1. Definition: $\mathrm{Hom}_R(M, N)$

1.2. Examples :

(i) $\mathrm{Hom}_R(R, M) \cong M$

(ii) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}) = \{0\}$ for any $n \neq 0$

(iii) If M is a torsion R-module, then $\mathrm{Hom}_R(M, R) = \{0\}$ (HW 6)

(iv) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n) \cong \mathbb{Z}_d$ where $d = (m, n)$. In particular, if $(m, n) = 1$, then $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n) = \{0\}$

(v) If V, W are k-vector spaces, then $\mathrm{Hom}_k(V, W)$ is the collection of linear transformations.

(vi) If (V, T) and (W, S) are $k[x]$-modules as before, then by Example II.2.2

$$\mathrm{Hom}_{k[x]}((V, T), (W, S)) = \{U \in \mathrm{Hom}_k(V, W) : UT = SU\}$$

1.3. Definition : Given $\theta : N \to N'$

(i) $\theta_* : \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N')$

(ii) $\theta^* : \mathrm{Hom}(N', M) \to \mathrm{Hom}(N, M)$

1.4. Remark/Example :

(i) Pictorial description of Definition 1.3

(ii) $(\theta \circ \varphi)_* = \theta_* \circ \varphi_*$ and $(\psi \circ \phi)^* = \phi^* \circ \psi^*$

(iii) Consider $\pi : \mathbb{Z} \to \mathbb{Z}_n$ to be the natural projection.

$$N = \mathbb{Z} \Rightarrow \pi^* = 0 \text{ since } \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}) = \{0\}$$
$$N = \mathbb{Z}_n \Rightarrow \pi^* = \mathrm{id}_{\mathbb{Z}_n} : \mathbb{Z}_n \to \mathbb{Z}_n \text{ (HW 6)}$$

(End of Day 22)

1.5. Lemma:

(i) $\mathrm{Hom}(M_1 \oplus M_2, N) \cong \mathrm{Hom}(M_1, N) \oplus \mathrm{Hom}(M_2, N)$

(ii) $\mathrm{Hom}(M, N_1 \oplus N_2) \cong \mathrm{Hom}(M, N_1) \oplus \mathrm{Hom}(M, N_2)$

1.6. Corollary: If M and N are free R-modules with $m = \mathrm{rank}(M), n = \mathrm{rank}(N)$, then $\mathrm{Hom}(M, N) \cong R^{mn}$

1.7. Definition :

(i) $\mathrm{End}_R(M)$

(ii) $\mathrm{Aut}_R(M)$

1.8. Examples: $\mathrm{Aut}_R(R/I) \cong (R/I)^*$

2. Exact Sequences

2.1. Definition:

(i) A pair of homomorphisms $\theta : A \to B$ and $\psi : B \to C$ forms a chain complex if $\psi \circ \theta = 0$; or equivalently, $\mathrm{Im}(\theta) \subset \ker(\psi)$

(ii) A pair of homomorphisms $\theta : A \to B$ and $\psi : B \to C$ is called exact at B if $\mathrm{Im}(\theta) = \ker(\psi)$. We denote this by $A \xrightarrow{\theta} B \xrightarrow{\psi} C$

(iii) An exact sequence $\ldots \to X_{n-1} \to X_n \to X_{n+1} \to \ldots$

2.2. Lemma:

(i) $0 \to A \xrightarrow{\theta} B$ is exact at A iff θ is injective

(ii) $A \xrightarrow{\psi} B \to 0$ is exact at B iff ψ is surjective

2.3. Corollary: $0 \to A \xrightarrow{\theta} B \xrightarrow{\psi} C \to 0$ is an exact sequence iff

(i) θ is injective

(ii) ψ is surjective

(iii) $\mathrm{Im}(\theta) = \ker(\psi)$

Such a sequence is called a short exact sequence.

2.4. Example:

(i) Let $\theta : M \to N$ be any homomorphism, then we have an exact sequence

$$0 \to \ker(\theta) \to M \xrightarrow{\theta} N \to N/\mathrm{Im}(\theta) \to 0$$

(ii) If $M = M_1 \oplus M_2$, we get a short exact sequence

$$0 \to M_1 \to M \to M_2 \to 0$$

(iii) If $0 \to V_1 \to V \to V_2 \to 0$ is an exact sequence of vector spaces, then $V \cong V_1 \oplus V_2$

(iv) Let $p \neq q \in \mathbb{Z}$ be prime numbers

(a) $0 \to \mathbb{Z}_p \to \mathbb{Z}_{pq} \to \mathbb{Z}_q \to 0$

(b) $0 \to \mathbb{Z}_p \to \mathbb{Z}_{p^2} \to \mathbb{Z}_p \to 0$

Both these sequences are exact, but

$$\mathbb{Z}_{pq} \cong \mathbb{Z}_q \oplus \mathbb{Z}_q \text{ but } \mathbb{Z}_{p^2} \ncong \mathbb{Z}_p \oplus \mathbb{Z}_p$$

(End of Day 23)

2.5. Definition: A submodule $N < M$ is called a direct summand of M if $\exists N' < M$ such that $N \oplus N' = M$

2.6. Theorem: For a short exact sequence $0 \to M_1 \xrightarrow{\theta} M \xrightarrow{\psi} M_2 \to 0$, TFAE :

(i) There exists a homomorphism $\alpha : M \to M_1$ such that $\alpha \circ \theta = 1_{M_1}$

(ii) There exists a homomorphism $\beta : M_2 \to M$ such that $\psi \circ \beta = 1_{M_2}$

(iii) $\mathrm{Im}(\theta) = \ker(\psi)$ is a direct summand of M

If these conditions hold, then

$$M \cong M_1 \oplus M_2$$

via the map $x \mapsto (\alpha(x), \psi(x))$.

2.7. Definition: If the conditions of Theorem 2.6 hold, then we say that the short exact sequence $0 \to M_1 \to M \to M_2 \to 0$ is a *split exact sequence.*

2.8. Remark: If $0 \to M_1 \xrightarrow{\theta} M \xrightarrow{\psi} M_2 \to 0$ is an exact sequence of R-modules, and N is any R-module, then

$$\mathrm{Hom}_R(N, M_1) \xrightarrow{\theta_*} \mathrm{Hom}_R(N, M) \xrightarrow{\psi_*} \mathrm{Hom}_R(N, M_2) \tag{0.1}$$

is a chain complex. Also,

$$\mathrm{Hom}_R(M_1, N) \xleftarrow{\theta^*} \mathrm{Hom}_R(M, N) \xleftarrow{\psi^*} \mathrm{Hom}_R(M_2, N) \tag{0.2}$$

is a chain complex. We ask whether these sequences are exact.

2.9. Theorem: For a short exact sequence $0 \to M_1 \xrightarrow{\theta} M \xrightarrow{\psi} M_2 \to 0$

In 0.1: (a) θ_* is injective

(b) $\ker(\psi_*) = \mathrm{Im}(\theta_*)$

(c) ψ_* may not be surjective

Hence,

$$0 \to \mathrm{Hom}_R(N, M_1) \xrightarrow{\theta_*} \mathrm{Hom}_R(N, M) \xrightarrow{\psi_*} \mathrm{Hom}_R(N, M_2)$$

is exact.

In 0.2: (a) ψ^* is injective

(b) $\ker(\theta^*) = \mathrm{Im}(\psi^*)$

(c) θ^* may not be surjective

Hence,

$$\mathrm{Hom}_R(M_1, N) \xleftarrow{\theta^*} \mathrm{Hom}_R(M, N) \xleftarrow{\psi^*} \mathrm{Hom}_R(M_2, N) \leftarrow 0$$

is exact

(End of Day 24)

2.10. Theorem: If $0 \to M_1 \xrightarrow{\theta} M \xrightarrow{\psi} M_2 \to 0$ is a split exact sequence, then the induced sequences

$$0 \to \mathrm{Hom}_R(N, M_1) \xrightarrow{\theta_*} \mathrm{Hom}_R(N, M) \xrightarrow{\psi_*} \mathrm{Hom}_R(N, M_2) \to 0$$

and

$$0 \leftarrow \mathrm{Hom}_R(M_1, N) \xleftarrow{\theta^*} \mathrm{Hom}_R(M, N) \xleftarrow{\psi^*} \mathrm{Hom}_R(M_2, N) \leftarrow 0$$

are both split exact.

3. Projective Modules

(See [Adkins, §3.5]) Assume all modules are f.g.

3.1. Lemma: Let F be a free R-module, then every short exact sequence

$$0 \to M_1 \to M \to F \to 0$$

is split exact.

3.2. Theorem: Let P be an R-module, then TFAE :

(i) Every short exact sequence

$$0 \to M_1 \to M \to P \to 0$$

is split exact

(ii) $\exists$ a free R-module F s.t. P is a direct summand of F

(End of Day 25)

3.3. Definition: Projective module

3.4. Examples :

(i) Free R-modules are projective

(ii) If $(m, n) = 1$, then $\mathbb{Z}_m$ is a projective $\mathbb{Z}_{mn}$-module, but it is not free.

(iii) If P_1, P_2 are projective, then $P_1 \oplus P_2$ is projective

(iv) Projective module is torsion free. Hence, a projective module over a PID must be free (by III.1.6)

(v) $R = \mathbb{Z}[\sqrt{-5}]$ and $I = \langle 2, 1 + \sqrt{-5} \rangle$, then I is projective, but not free.

3.5. Definition: Invertible ideal

3.6. Theorem: Let R be an integral domain, and $I \lhd R$. Then I is a projective R-module iff I is invertible.

(End of Day 26)

3.7. Examples:

(i) Every non-zero principal ideal is invertible

(ii) If $R = \mathbb{Z}[\sqrt{-5}]$ and $I = \langle 2, 1 + \sqrt{-5} \rangle$, then I is invertible.

3.8. Remark: A Dedekind domain is an integral domain in which every ideal is invertible. All PIDs are Dedekind domains, and $\mathbb{Z}[\sqrt{-5}]$ is Dedekind domains that is not even a UFD. Dedekind domains are important in number theory.

4. Noetherian Rings

4.1. Definition: R is Noetherian if every ideal is f.g.

4.2. Examples:

(i) Fields, Division Rings, Finite rings

(ii) PIDs

(iii) $C_b(\mathbb{R})$ is not Noetherian (Example I.4.5)

4.3. Lemma: R is Noetherian iff every increasing sequence $I_1 \subset I_2 \subset \dots$ of ideals is stationary. ie. $\exists k \in \mathbb{N}$ such that $I_n = I_k$ for all $n \geq k$

4.4. (Hilbert Basis Theorem): If R is Noetherian, then $R[x]$ is a Noetherian ring.

4.5. Corollary: If k is a field, then the polynomial ring $k[x_1, x_2, \dots, x_n]$ in n variables is Noetherian.

4.6. Example: If $V = \{(0,0), (0,1), (1,0)\} \subset \mathbb{C}^2$, and $I \lhd \mathbb{C}[x,y]$ is the ideal

$$I = \{f(x,y) \in \mathbb{C}[x,y] : f(p,q) = 0 \quad \forall (p,q) \in V\}$$

Then $I = \langle x^2 - x, xy, y^2 - y \rangle$

(End of Day 27)

4.7. Definition:

(i) If $S \subset k^n$, write $I(S) := \{f \in k[x_1, x_2, \dots, x_n] : f(a) = 0 \quad \forall a \in S\}$

Example: If $S = \{(0,0), (0,1), (1,0)\}$, then $I(S) = \langle x^2 - x, xy, y^2 - y \rangle$

(ii) If $I \lhd k[x_1, x_2, \dots, x_n]$, write $V(I) = \{a \in k^n : f(a) = 0 \quad \forall f \in I\}$.

Example: $I = \langle x^2 - y \rangle$, then $V(I) = \{(x,y) : y = x^2\}$

(iii) Hypersurface is $V(\langle f \rangle) =: V(f)$ for some $f \in k[x_1, x_2, \dots, x_n]$

4.8. Remark:

(i) Every algebraic set is the intersection of finitely many hypersurfaces

(ii) $I(S) \lhd k[x_1, x_2, \dots, x_n]$

(iii) $I \subset I(V(I))$

(iv) For $0 \neq a \in \mathbb{C}$, and $I = \langle y^2 - x, x - a \rangle$, we have $I = I(V(I))$

(v) If $0 = a \in \mathbb{C}$, and $I = \langle y^2 - x, x \rangle$, we have $I \neq I(V(I)) = \langle x, y \rangle$. Note that $y \in J \setminus I$, but $y^2 \in I$

4.9. (Hilbert Nullstellensatz): If $I \lhd \mathbb{C}[x_1, x_2, \dots, x_n]$, then

$$I(V(I)) = \{f \in k[x_1, x_2, \dots, x_n] : \exists n \in \mathbb{N} \text{ such that } f^n \in I\}$$

(without proof)

Note:

(i) This is called the radical of I, and is denoted by $\sqrt{I}$

(ii) If $I = \{0\}$, then $\sqrt{0}$ is the set if nilpotent elements.

4.10. Lemma: If R is Noetherian, and $I \lhd R$, then R/I is Noetherian.

4.11. Example: $\mathbb{Z}[\sqrt{-5}]$ is Noetherian. In particular, as in HW 2.4, $\mathbb{Z}[\sqrt{-5}]$ satisfies **(UF1)** (Every non-zero non-unit is a product of irreducible elements)

(End of Day 28)

5. Noetherian Modules

(See [Musili, §6.2])

5.1. Definition: A module M is called *Noetherian* if every submodule of M is f.g. (In particular, M is f.g.)

5.2. Examples:

(i) A ring is Noetherian iff it is Noetherian as a module over itself.

In particular, $C_b(\mathbb{R})$ is not Noetherian as a $C_b(\mathbb{R})$ module (See Example I.4.5)

(ii) $R[x]$ is not Noetherian as an R-module

(iii) A module M over a PID if Noetherian iff M is f.g. (See III.1.4)

In particular, a finitely generated abelian group is Noetherian.

A vector space is Noetherian as a k-module iff it is finite dimensional.

(iv) $\mathbb{Q}/\mathbb{Z}$ is not Noetherian as a $\mathbb{Z}$-module since it is not f.g. (Mid-Sem Exam # 3)

5.3. Prop: Let M be Noetherian, and $N < M$, then

(i) N is Noetherian

(ii) M/N is Noetherian

5.4. Prop: If M is a module and $N < M$ is s.t. N and M/N are Noetherian, then M is Noetherian.

5.5. Theorem:

(i) If $M_1, M_2, \ldots, M_k$ are Noetherian, then $M_1 \oplus M_2 \oplus \ldots \oplus M_k$ is Noetherian.

(ii) In particular, if R is Noetherian, then R^n is Noetherian

5.6. Corollary: If R is Noetherian, a module over R is Noetherian iff it is f.g.

5.7. Theorem: M is Noetherian R-module iff every increasing chain of submodules is stationary. (See Lemma 4.3)

6. Artinian Modules

(See [Musili, §6.1])

6.1. Definition: Artinian module

6.2. Examples:

(i) If V is a vector space, then V is Artinian iff $\dim(V) < \infty$

(ii) A finite abelian group is Artinian

(iii) $\mathbb{Z}$ is not Artinian.

(iv) $\mathbb{Z}(p^\infty)$ is Artinian, but not Noetherian (See HW 5.9)

(End of Day 29)

6.3. Prop: Submodules and Quotients of Artinian modules are Artinian.

6.4. Prop: If M is a module and $N < M$ is a submodule s.t. N and M/N are Artinian, then M is Artinian.

6.5. Theorem:

(i) If $M_1, M_2, \ldots, M_k$ are Artinian, then $M_1 \oplus M_2 \oplus \ldots \oplus M_k$ is Artinian.

(ii) In particular, if R is Artinian, then R^n is Artinian.

6.6. Corollary:

(i) If R is Artinian and M is a f.g. R-module, then M is Artinian.

(ii) An Artinian module need not be f.g. though (Example : $\mathbb{Z}(p^\infty)$)

6.7. Theorem: Let R be an Artinian ring

(i) If R is an integral domain, then R is a field.

(ii) Every prime ideal of R is a maximal ideal.

7. Length of a module

(See [Musili, §6.3])

7.1. Definition:

(i) Simple module

(ii) Maximal submodule

(iii) Minimal submodule

7.2. Remark/Examples:

(i) M is simple iff $M \cong R/I$ for some maximal ideal $I \lhd R$ (with proof)

(ii) Let V be a k-vector space, then

(a) V is simple iff V is one-dimensional

(b) A subspace $W \subset V$ is maximal iff $\dim(V/W) = 1$. If V is finite dimensional, then this is the same as saying that $\dim(W) = \dim(V) - 1$

(c) A subspace $W \subset V$ is minimal iff $\dim(W) = 1$

(iii) (a) $\mathbb{Z}_p$ is a simple $\mathbb{Z}$-module. In fact, this is the only simple $\mathbb{Z}$-module

(b) $p\mathbb{Z} \lhd \mathbb{Z}$ are the only maximal submodules of $\mathbb{Z}$

(c) $\mathbb{Z}$ has no minimal submodules, since for any $n \in \mathbb{Z}$, $(n) \supset (2n)$

(iv) Let $M = \mathbb{Z}(p^\infty)$, then

(a) M is not simple

(b) M has no maximal submodules

(c) $C_1 = \langle \overline{1/p} \rangle$ is a minimal submodule

(End of Day 30)

7.3. Lemma: Let M be an R-module

(i) If M is Noetherian, then M has a maximal submodule

(ii) If M is Artinian, then M has a minimal submodule

7.4. Definition: Composition Series

Note: If M has a composition series, then M has both a maximal and a minimal submodule.

7.5. Examples:

(i) A k-vector space V has a composition series iff $\dim(V) < \infty$ (with proof)

(ii) A finite abelian group has a composition series.

(iii) $\mathbb{Z}$ does not have a composition series

(iv) $\mathbb{Z}(p^\infty)$ does not have a composition series, even though it has a minimal submodule.

7.6. Theorem: M has a composition series iff M is both Artinian and Noetherian.

7.7. Corollary: Let M be a module and $N < M$. Then M has a composition series iff N and M/N both have composition series.

(End of Day 31)

7.8. (Jordan-Hölder Theorem): If M has two composition series

$$M = M_0 \supset M_1 \supset M_2 \supset \ldots \supset M_m = \{0\} \text{ and}$$

$$M = N_0 \supset N_1 \supset N_2 \supset \ldots \supset N_n = \{0\}$$

then

(i) $n = m$

(ii) For all $1 \leq i < m, \exists 1 \leq j < n$ such that $M_i/M_{i+1} \cong N_j/N_{j+1}$

7.9. Definition: Length of a module M, denoted by $\ell(M)$

7.10. Remark/Examples:

(i) $\ell(M) \geq 0$ and $\ell(M) = 0$ iff $M = \{0\}$

(ii) $\ell_R(M) = 1$ iff M is simple. In general, $\ell(M)$ is the departure of M from being simple.

(iii) If G is a finite abelian group and $|G| = p_1 p_2 \dots p_k$ (where the p_i are not necessarily distinct primes), then $\ell(G) = k$

(iv) If V is a k-vector space, then $\ell(V) = \dim(V)$

7.11. Theorem: Let M be an R-module and $N < M$. Then $\ell(M) = \ell(N) + \ell(M/N)$

7.12. Corollary: If $M := M_1 \oplus M_2 \oplus \dots \oplus M_k$, then $\ell(M) = \sum_{i=1}^{n} \ell(M_i)$

7.13. Corollary: Let V be a k-vector space, then TFAE :

(i) V is finite dimensional

(ii) V has finite length

(iii) V is Noetherian as a k-module

(iv) V is Artinian as a k-module

If any of these conditions are satisfied, then any two bases of V have the same number of elements, and $\ell(V) = \dim(V)$

(End of Day 32)

V. Tensor Products

1. Finite Dimensional Vector Spaces

(See [Gowers])

Let U, V, W, X, etc. denote finite dimensional vector spaces over a field k

1.1. Definition: Bilinear map $f : V \times W \to X$

1.2. Examples:

(i) If V is an inner product space over $\mathbb{R}$, then the inner product $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ is bilinear.

(ii) Cross product $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$

(iii) If V is a vector space, and V^* its dual, then $B : V \times V^* \to k$ defined by $B(v, f) := f(v)$ is bilinear.

(iv) $\psi : \mathbb{C} \times \mathbb{R}^n \to \mathbb{C}^n$ given by $(z, \overline{v}) \mapsto (zv_1, zv_2, \dots, zv_n)$

1.3. Remark:

(i) A linear map $T : V \to W$ can be encoded in a matrix $[T]_{\mathcal{B}}$ for some basis $\mathcal{B}$ of V. Similarly, a bilinear map $f : V \times W \to X$ can be encoded in a 3-dimensional $n \times m \times r$ grid, whose $(i, j, k)^{th}$ entry is the k^{th} coordinate of $f(v_i, w_j)$ where $\{v_i\}$ and $\{w_j\}$ are bases of V and W respectively.

Question: Can we instead encode f in a matrix? In other words, we need a suitable set S of vectors such that $[f]_S$ captures f uniquely.

(ii) If $V = W = X = \mathbb{R}$, then $S = \{(1,0),(0,1)\}$ forms a basis for $V \times W$, but $[f]_S$ is zero, and does not give any information regarding f. However, if $0 \neq a, 0 \neq b$, then $S = \{(a,b)\}$ is not a basis for $V \times W$, but $f(a,b)$ gives all the information we need about f since $f(x,y) = \frac{xy}{ab} f(a,b)$ for any bilinear f

(iii) Any $f : V \times W \to X$ is determined by $f = (f_1, f_2, \ldots, f_r)$ where $f_i : V \times W \to k$ are all bilinear.

1.4. Definition:

(i) $B_k(V,W)$ is the vector space of all bilinear maps $f : V \times W \to k$

(ii) For $v \in V, w \in W$, define $v \otimes w : B_k(V,W) \to k$ by $v \otimes w(f) := f(v,w)$. Notice that $v \otimes w \in B_k(V,W)^*$, the dual space of $B_k(V,W)$

(iii) Define $V \otimes W := \text{span}\{v \otimes w : v \in V, w \in W\}$

1.5. Theorem: If $\{v_i\}$ and $\{w_j\}$ are bases for V and W respectively, then $\{v_i \otimes w_j\}$ is a basis for $V \otimes W$. In particular, $\dim(V \otimes W) = \dim(V) \times \dim(W)$

1.6. Lemma: The map $\varphi : V \times W \to V \otimes W$ given by $\varphi(v,w) := v \otimes w$ is bilinear.

1.7. Proposition: If X is a finite dimensional vector space, and $g : V \times W \to X$ is a bilinear map, then $\exists! T : V \otimes W \to X$ linear such that $T \circ \varphi = g$. In other words, there is an isomorphism

$$B_X(V,W) \cong \text{Hom}_k(V \otimes W, X)$$

(End of Day 33)

1.8. Theorem: The pair $(V \otimes W, \varphi)$ is unique in the following sense : If U is a finite dimensional vector space and $\psi : V \times W \to U$ is a bilinear map such that, for any bilinear map $h : V \times W \to X$, $\exists! S : U \to X$ such that $S \circ \psi = h$, then there is an isomorphism $\mu : U \to V \otimes W$ such that $\mu \circ \psi = \varphi$

1.9. Example:

(i) $\mathbb{C} \otimes \mathbb{R}^n \cong \mathbb{C}^n$

(ii) $V \otimes V^* \cong \text{End}_k(V)$

(iii) If $\psi : V \times V^* \to k$ is given by $(v,f) \mapsto f(v)$, then the induced linear map $S : \text{End}_k(V) \to k$ is the trace.

2. Tensor Product of Modules

Note: If M and N are modules, then $M \otimes N$ cannot follow the same idea as above, because if M has torsion, then $B_R(M,N) = \{0\}$

2.1. Definition for modules (in terms of universal property)

2.2. Theorem: The tensor product (T, φ), if it exists, is unique.

2.3. Examples:

(i) $R \otimes_R M \cong M$

(ii) $\mathbb{Z}_a \otimes_{\mathbb{Z}} \mathbb{Z}_b \cong \mathbb{Z}_d$ where $d = (a, b)$

In particular, if $(a, b) = 1$, then $\mathbb{Z}_a \otimes_{\mathbb{Z}} \mathbb{Z}_b = \{0\}$

(End of Day 34)

2.4. Remark: (The construction of $M \otimes_R N$)

(i) Let F be the free module on $M \times N$

(ii) Let H be the subgroup generated by

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

(iii) Define $T := F/H$ and $\varphi : M \times N \to T$ by $(m, n) \mapsto (m, n) + H$

2.5. Theorem: The pair (T, φ) is a tensor product of M and N. We write $T = M \otimes_R N$ and $m \otimes n := \varphi(m, n)$

2.6. Theorem:

$$(M_1 \oplus M_2) \otimes N \cong (M_1 \otimes N) \otimes (M_2 \otimes N)$$
$$M \otimes (N_1 \otimes N_2) \cong (M \otimes N_1) \oplus (M \otimes N_2)$$

2.7. Examples:

(i) $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q} = \{0\}$

So, If G is any finite abelian group, then $G \otimes \mathbb{Q} = \{0\}$

(ii) $\mathbb{Z}^n \otimes \mathbb{Q} \cong \mathbb{Q}^n$ (Similar to Example 1.9(ii))

If G is a finitely generated abelian group, then $G \otimes \mathbb{Q}$ is a $\mathbb{Q}$-vector space whose dimension is the free-rank of G

(iii) More generally, if M is a f.g. module over a PID R, and $K = \text{Quot}(R)$, then $M \otimes K$ is a K-vector space whose dimension os the free-rank of M

2.8. Corollary: If M and N are free R-modules of rank m and n respectively, then $M \otimes N$ is a free module of rank mn

(End of Day 35)

2.9. Remark: (Extension of Scalars)

(i) If $R \subset S$ are two rings, and M is an S-module, then M is also an R-module. But if M is an R-module, then can M be made into an S-module?

(ii) Example:

(a) $\mathbb{Z}$ is a $\mathbb{Z}$-module, but cannot be made into a $\mathbb{Q}$-module: If it could, then $x = \frac{1}{2} \cdot 1 \in \mathbb{Z}$ would satisfy $2x = 1$ which is impossible. However, $\mathbb{Z}$ is contained in a $\mathbb{Q}$-module, namely $\mathbb{Q}$ itself.

(b) If $M = \mathbb{Z}/2\mathbb{Z}$ is a $\mathbb{Z}$-module, then M does not embed in any $\mathbb{Q}$-module, because if N is any $\mathbb{Q}$-module and $f : M \to N$ any embedding, then $2f(x) = 0$ for all $x \in M$, and hence $\frac{1}{2} \cdot 2f(x) = 0 \Rightarrow f \equiv 0$

(iii) The map $S \times S \otimes M \to S \otimes M$ given by

$$(s, \sum_{i=1}^{n} s_i \otimes m_i) \mapsto \sum_{i=1}^{n} (ss_i) \otimes m$$

makes $S \otimes M$ into an S-module.

2.10. Theorem: Let $\iota : M \to S \otimes M$ be the map $m \mapsto 1_S \otimes m$. If N is any S-module (and hence R-module), and $\theta : M \to N$ a homomorphism of R-modules, then $\exists! T : S \otimes M \to N$ such that $T \circ \iota = \theta$. Hence,

$$\mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_S(S \otimes M, N)$$

Review of Chapter I

(End of Day 36)

Review of Chapter II, III, IV

(End of Day 37)

Review of Chapter IV, V

(End of Day 38)

VI. Instructor Notes

0.1. Doing Chinese Remainder theorem in this course (as against MTH 301) was hugely beneficial. It supports the structure theorem for modules, and helps understand the transition between invariant factors and elementary divisors. Doing it in MTH 301 would not have been as helpful.

0.2. I discussed Rational/Jordan canonical forms as an important application of the structure theorem because it hadn't been covered in Advanced Linear Algebra, and also because it served as an important example throughout the course.

0.3. I discussed composition series because I wanted them to see Jordan-Hölder once before seeing it in Galois theory when discussing solvable groups. We will see next semester if this was beneficial or not.

0.4. I did not discuss non-commutative rings - Schur's Lemma,etc - but decided to focus on commutative algebra in the form of Noetherian/Artinian modules instead. I believe the course flows better this way, but perhaps if I had had more lectures (we lost many due to various holidays), I would have been able to discuss non-commutative rings as well.

0.5. Although I discussed tensor products, it was woefully inadequate. Perhaps it was my fault, but I think they are a little too abstract for this point in the students' education. Not sure it should be there in this course.

Bibliography

[Norman] Christopher Norman, *Finitely Generated Abelian groups and Similarity of Matrices over a Field*

[Hartley] Hartley and Hawkes, *Rings, Modules and Linear Algebra*

[Adkins] Adkins and Weintraub, *Algebra : An approach via Module theory*

[Dummit] Dummit and Foote, *Abstract Algebra*

[Lang] S. Lang, *Algebra, Revised 3rd Ed.*

[Musili] C. Musili, *Introduction to Rings and Modules, 2nd Revised Edition*

[Gowers] T. Gowers, How to lose your fear of tensor products (Online Notes)