MAT 250B: Abstract Algebra

Greg DePaul

April 24, 2021

1 Rings

1.1 Initial Definitions

Definition 1.1. *A ring R is a set with two binary operations $+, \cdot$ such that*

1. *$(R, +)$ is an Abelian group*
2. *$\cdot$ is associative*
3. *$\cdot$ has an identity $1 \in R$ (That is, we assume all rings are unital)*
4. *Distributivity:*

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

for all $a, b, c \in R$

If $\cdot$ is commutative, we call R commutative.

Example 1.2. *$R = \mathbb{Z}$ with 0 additive and 1 multiplicative.*

Example 1.3. *$R = \mathbb{Z}/n\mathbb{Z}$*

Example 1.4. *$R = \mathbb{M}_3(\mathbb{C})$ is not commutative!*

Example 1.5. *$R = \mathbb{Q}$*

Example 1.6. *$R = \mathbb{Q}[\mathbb{S}_3]$ is a group ring! We define it to be similar to a vector space, with*

$$R = \mathbb{Q}[\mathbb{S}_3] = \left\{ \sum a_\sigma \sigma : a_\sigma \in \mathbb{Q}, \sigma \in \mathbb{S}_3 \right\}$$

where $\mathbb{S}_n :=$ is the symmetric group over n elements! Underlying space is a $\mathbb{Q}$ vector space with basis $\mathbb{S}_3$.

Proposition 1.7. *Let R be a ring with $a \in R$*

1. *$0 \cdot a = a \cdot 0 = 0$*
2. *$1 = 0$ if and only if $R = \{0\}$, the zero ring.*
3. *$-a = (-1) \cdot a = a \cdot (-1)$. Also $(-1) \cdot (-a) = a = (-a) \cdot (-1)$*
4. *For $n \in \mathbb{N} = \mathbb{Z}_{\geq 0}$ if*

$$n = n \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{n} = 0$$

Then $n \cdot a = 0$

Definition 1.8. *Let R be a ring. A subset $S \subset R$ is a subring if*

1. *$1 \in S$*

2. $(S,+) \leqslant (R,+)$

3. $a,b \in S \implies a \cdot b \in S$

Example 1.9. *$R = \mathbb{M}_2(\mathbb{F}_3)$. In this case,*

$$3 \cdot I = 3 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \bar{3} & 0 \\ 0 & \bar{3} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Remark 1.10. *Subrings aren't particularly interesting. Instead, it's ideals that are really interesting to study.*

Definition 1.11. *Let R be a ring . A subset $I \subset R$ is an <u>ideal</u> if*

1. $(I,+) \leqslant (R,+)$

2. *For all $a \in I, r \in R, a \cdot r \in I, r \cdot a \in I$. (Absorption Property)*

It's important to specify the absorption property on both sides:

- If just $ra \in I$, we call I a <u>left ideal</u>
- If just $ar \in I$, we call I a <u>right ideal</u>

So the definition above would be also called a <u>2-sided ideal</u>.

Example 1.12. *Let $R = \mathbb{M}_3(\mathbb{C})$. Consider S to be the set of upper triangular matrices. Then S is a perfectly good subring.*

Example 1.13. *Let $R = \mathbb{M}_3(\mathbb{C})$. Consider S to be the set of uni-upper triangular matrices (ones along the diagonal). Then S fails to be a subring since adding two elements would give 2s along the diagonal .*

Example 1.14. *Let $R = \mathbb{M}_3(\mathbb{C})$ with $S = M_3(\mathbb{Z})$. Then this is a perfectly acceptable subring.*

Example 1.15. *Let $R = \mathbb{M}_3(\mathbb{C})$ and consider S to be the set of upper triangular matrices. Then S <u>cannot</u> be an ideal since it contains the identity!*

Lemma 1.16. *If I is an ideal and $1_R \in I$, then $I = R$.*

Proof. By the absorption property, take any $r \in R$.. Then we see that since $1 \in I, r \cdot 1 \in I \implies R \subset I \implies I = R$. ∎

Example 1.17. *Let $R = \mathbb{M}_3(\mathbb{C})$ and consider*

$$I := \left\{ \begin{pmatrix} * & * & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right\}$$

This this forms a right ideal! But it is not what we call an ideal.

Example 1.18. *$R = \mathbb{C}[x]$ and let $S = \mathbb{Q}[x]$. Then S is a subring.*

Example 1.19. *$R = \mathbb{C}[x]$ and consider $I = \{f(x) \in \mathbb{C}[x] : f(2) = 0\}$. Then I is an ideal, and moreover, it's a principal ideal and can be written $I = \langle x - 2 \rangle$.*

Example 1.20. *$R = \mathbb{C}$ and let $S = \mathbb{Z}[i]$. Then S is a subring! Clearly, it cannot be an ideal*

Example 1.21. *$R = \mathbb{C}$. Then $I = \{0\}$ is the trivial ideal. It however fails to be a subring under the multiplication operation defined on the ambient space R.*

Example 1.22. *$R = \mathbb{Z}[i]$. Also $I = 2\mathbb{Z}$ is not an ideal.*

Definition 1.23. *Let R, S be rings. A function $\phi : R \to S$ is a <u>ring homomorphism</u> provided:*

1. $\phi(1_R) = 1_S$
2. *For all* $a, b \in R, \phi(a+b) = \phi(a) + \phi(b)$
3. *For all* $a, b \in R, \phi(a \cdot b) = \phi(a) \cdot \phi(b)$

Example 1.24. *Consider*

$$\begin{aligned} \phi : \mathbb{Z} &\to \mathbb{Z} \\ a &\to 2a \end{aligned}$$

is a perfectly good group homomorphism, but fails to be a ring homomorphism. We can see this because the image of a homomorphism ϕ *should be a subring, which* $2\mathbb{Z}$ *fails to be since it doesn't possess the identity.*

Example 1.25. *Consider*

$$\begin{aligned} \phi : \mathbb{Z}[x] &\to \mathbb{R} \\ f(x) &\to f(2) \end{aligned}$$

Proposition 1.26. *Let* $\phi : R \to S$ *be a ring homomorphism. Then* $Ker\phi$ *is an ideal of* R*, where*

$$Ker\phi := \{a \in R : \phi(a) = 0\} = \phi^{-1}(0_R)$$

Proof. Left as exercise. ■

Definition 1.27. *Let* R *be a ring,* $I \subset R$ *an ideal. Then* R/I *is the quotient ring, with well-defined operations:*

$$(a+I) + (b+I) = (a+b) + I$$

$$(a+I) \cdot (b+I) = a \cdot b + I$$

with $1 + I$ *the identity.*

Example 1.28. *If* R *is a ring and* $\phi : \mathbb{Z} \to R$ *a homomorphism, we must have* $\phi(1) = 1_R$*. So* ϕ *is unique, with* $Ker\phi = n\mathbb{Z}$ *for some* n*. If we take* $n \geq 0$*, then* $n :=$ *characteristic of* R *with* $Im\phi \cong \mathbb{Z}/n\mathbb{Z}$*. In essence, we can embed the integers in every ring.*

Question 1.29. *What are all the ideals of* $\mathbb{Z}$*?*

Definition 1.30. *Let* R *be a commutative ring with* $a \in R$*. Then principal ideal generated by* a *is*

$$\langle a \rangle := \{ra : r \in R\}$$

This is an ideal, and it is in fact the smallest ideal of R containing a with

$$\langle a \rangle := \bigcap_{a \in I \subset R} I$$

Question 1.31. *If* R *is not commutative, what is* $\langle a \rangle$*? In the non-commutative setting, we want this to be a two-sided ideal.*

Example 1.32. *In* $R = M_2(\mathbb{Q})$ *with* $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$*, then* $\langle a \rangle = R$*.*

Remark 1.33. *If* R *is not commutative, then we can think of the left ideal generated by to simply be* $Ra = \{ra : r \in R\}$ *and similarly for the right ideal.*

1.2 The Isomorphism Theorems

Theorem 1.34 (The First Isomorphism Theorem)**.** *Let $\phi : R \to S$ be a ring homomorphism with kernel $J = Ker(\phi)$. Then $Im(\phi) \cong R/J$. In particular, any ideal is a kernel!*

Theorem 1.35 (The Second Isomorphism Theorem)**.** *Let R be a ring, $S \subset R, I \subset R$ an ideal. Note $S \cap I \subset I$ is an ideal and*

$$S/S \cap I \cong (S + I)/I$$

In particular, $S + I$ is a subring.

Note 1.36. *$(S + I)/I \subset R/I$ is a subring.*

Theorem 1.37 (Correspondence Theorem)**.** *Let $I \subset R$ be an ideal. Then there exist the bijections*

$$\begin{aligned} \{\textit{subrings of } R/I\} &\iff \{\textit{subrings } A \subset R \textit{ with } I \subset A \subset R\} \\ \{\textit{ideals of } R/I\} &\iff \{\textit{ideals } J \subset R \textit{ with } I \subset J \subset R\} \\ J/I &\iff J \textit{ with } \pi^{-1}(J/I) \end{aligned}$$

where π is the projection map defined:

$$\begin{aligned} \pi : R &\to R/I \\ a &\to a + I \end{aligned}$$

Theorem 1.38 (The Third Isomorphism Theorem)**.** *Let R be a ring with ideals $I \subset K \subset R$. Recall $J/I = \{a+I : a \in J\}$ is an ideal of R/I. Then*

$$(R/I)/(J/I) \cong R/J$$

Example 1.39. *Consider $12\mathbb{Z} \subset 4\mathbb{Z} \subset \mathbb{Z}$. Then we have*

$$4\mathbb{Z}/12\mathbb{Z} \subset \mathbb{Z}/12\mathbb{Z}$$

and by the third isomorphism theorem

$$(\mathbb{Z}/12\mathbb{Z})/(4\mathbb{Z}/12\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$$

Example 1.40. *Consider the homomorphism on the polynomial ring*

$$\begin{aligned} \phi : \mathbb{Q}[x] &\to \mathbb{Q} \\ f(x) &\to f(2) \end{aligned}$$

Then we see

$$Im(\phi) = \mathbb{Q}$$

$$Ker(\phi) = \langle x - 2 \rangle$$

By the first isomorphism theorem, we see:

$$\mathbb{Q}[x]/\langle x - 2 \rangle \cong \mathbb{Q}$$

Example 1.41. *Consider the homomorphism on the polynomial ring*

$$\begin{aligned} \psi : \mathbb{Q}[x] &\to \mathbb{C} \\ f(x) &\to f(i) \end{aligned}$$

1.3 Units, Domains and Fields

Definition 1.42. *An element $u \in R$ is a unit provided there exists $v \in R$ such that $uv = vu = 1_R$. The collection of units is often denoted $\{u \in R : u \text{ is a unit}\} = U(R) = \mathbb{R}^\times$.*

Example 1.43. $\mathbb{Z}^\times = \{\pm 1\}$

Example 1.44. $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

Proposition 1.45. $\mathbb{R}^\times$ *is a group under multiplication.*

Example 1.46. $\mathbb{M}_3(\mathbb{R})^\times = GL_3(\mathbb{R})$, *the invertible 3×3 matrices.*

Exercise 1.47. *Describe the elements of $M_3(\mathbb{Z})^\times$?*

Definition 1.48. *Let R be commutative. Take element $a, b \in R$. Then a divides b, with $a|b$, if there exists c such that $b = ac$.*

Note 1.49. $u \in R^\times \iff a|1$.

Definition 1.50. *$a \in R$ is a zero-divisor if $a \neq 0$ and there exists $b \neq 0$ such that*

$$a \cdot b = 0$$

Notationally, we can write this as $a|0$.

Definition 1.51. *R is a domain if it has no-zero divisors.*

Definition 1.52. *R is an integral domain if it is a commutative domain.*

Definition 1.53. *A field is a commutative ring $\mathbb{F}$ such that $F \neq \{0\}$ and $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$.*

Note 1.54. *If $\mathbb{F}$ is a field then $\mathbb{F}$ is an integral domain.*

We can talk about a non-commutative analogue of fields, called a division ring (or skew field)

Example 1.55. *The Real Quaternions or Hamiltonions is defined by*

$$\mathbb{H} := \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

where

$$i^2 = j^2 = k^2 = -1 \quad \text{and} \quad ij = j = -ji$$

We can define conjugation in the quaternions to be:

$$z = a + bi + cj + dk \implies \bar{z} = a - bi - cj - dk$$

$$z\bar{z} = a^2 + b^2 + c^2 + d^2$$

which allows us to identify inverses of $(a, b, c, d) \neq (0, 0, 0, 0)$ by

$$z^{-1} = \frac{\bar{z}}{a^2 + b^2 + c^2 + d^2}$$

Notice that $\mathbb{H} \neq \mathbb{R}[Q_8]$, which is a group ring. Recall

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

Moreover, we see that because $Z(Q_8) = \{1, -1\}$, then we see

$$\mathbb{H} \cong R[Q_8]/\langle (-1) \cdot 1 = -1 \rangle$$

Warning: If G is Abelian, we may want to write multiplicatively $\cdot$ not additively $+$.

Example 1.56. $\mathbb{R}[\mathbb{Z}/n\mathbb{Z}]$ *the operation of the group is different than that of the ring.*

Proposition 1.57. $\mathbb{Z}/n\mathbb{Z}$ *is a field if and only if* n *is prime.*

Proposition 1.58. $\mathbb{Z}/n\mathbb{Z}$ *is an integral domain if and only if* n *is prime.*

Notice, if $a \in \mathbb{Z}/n\mathbb{Z}$, then $a = 0$, or $a \in a \in (\mathbb{Z}/n\mathbb{Z})^\times$ or a is a zero-divisor.

Proposition 1.59. *If* R *is a finite integral domain, then* R *is a field.*

Proof. Let $a \in R \setminus \{0\}$. Consider the function

$$\begin{aligned} f : R &\to R \\ r &\to ar \end{aligned}$$

First, we claim that f is injective: If $ar = as \implies a(r-s) = 0 \implies r - s = 0 \implies r = s$. Since $|R| < \infty$, then f injective also implies f is surjective. So there exists $t \in R$ such that

$$ta = at = f(t) = 1 \implies a \in R^\times$$

Since this is true for all $a \in R \implies R$ is a field! ■

Proposition 1.60. *Let* R *be a domain. Then its characteristic is 0 or some prime* p*.*

Proposition 1.61. *Let* R *be an integral domain. Then* $(R[x])^\times = \mathbb{R}^\times$*.*

Proof. Homework. ■

Proposition 1.62. *If* I, J *are ideals, then* $IJ = \{\sum_k a_k b_k : a_k \in I, b_k \in J\}$ *is an ideal.*

Proof. Homework. ■

Proposition 1.63.

$$\langle a \rangle = RaR = \left\{ \sum_k r_k a s_k : r_k, s_k \in R \right\}$$

Proposition 1.64. *Let* R *be commutative,* $M \subset R$ *be an ideal. Then* M *is maximal if and only if* R/M *is a field.*

Note 1.65. *Maximal implies* $M \neq R$ *so* $R = \{0\}$ *is not considered.*

Proposition 1.66. *Let* R *be commutative.* R *is a field if and only if* R *has exactly ideals. These ideals must be specifically* $\langle 0 \rangle$ *and* $R = \langle 1 \rangle$*.*

Proof. Proof on your own time. ■

Definition 1.67. *Let* R *be a commutative ring. An ideal* $P \subset R$ *is a* <u>*prime ideal*</u> *if* $P \neq R$ *and* $ab \in P \implies a \in P$ *or* $b \in P$*.*

In grade school, we're usually taught the definition of irreducibility in place of the definition of prime.

Proposition 1.68. *Let* R *be a commutative ring. Then* $P \subset R$ *is prime if and only if* R/P *is an integral domain.*

1.4 Rings of Fractions

Recall, you can "build" $\mathbb{Q}$ from $\mathbb{Z}$ be defining $\mathbb{Z} \setminus \{0\} = D$. We can define the set of ordered pairs $\mathbb{Z} \times D/\ $ where the relation $\ $ is defined by

$$(a, b)\ (c, d) \iff ad = bc$$

If $b \neq 0$, then we simply denote the pair (a, b) by $\frac{a}{b}$. Notice, $\frac{a}{b} = \frac{ak}{bk}$.
Now, we can define $+, \cdot$ accordingly and how $\mathbb{Z}$ embeds within this new ring. Can repeat with $\mathbb{Z}$ replaced by any integral domain to get the field of fractions.

We can also generalize this if we make D smaller, or not domain if D "nice" or not commutative (Ore).

Example 1.69. *Let $\mathbb{F}$ be a field with $R = \mathbb{F}[x]$. Then we can consider the field of fractions of*

$$R := \mathbb{F}(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}[x], g(x) \neq 0 \right\}$$

Note 1.70. *$\mathbb{F}_5(x)$ is an infinite field of finite characteristic.*

Example 1.71. *You saw in the homework, we saw the Formal Power Series $\mathbb{F}[[x]]$ and, in fact, $R[[x]]$ for any commutative ring, we define*

$$\mathbb{F}[[x]] = \left\{ \sum_{i=0}^{\infty} a_i x^i : a_i \in \mathbb{F} \right\}$$

with units

$$(\mathbb{F}[[x]])^{\times} = \left\{ \sum_{i=0}^{\infty} a_i x^i : a_i \neq 0 \right\}$$

We can also identify $\mathbb{F}[[x]]$ with functions $\{\sigma : \mathbb{N} \to \mathbb{F}\}$ by

$$\sum_{i=0}^{\infty} a_i x^i \leftrightarrow \sigma(i) = a_i$$

equipped with component-wise addition and multiplication defined by :

$$(\sigma\tau)(i) = \sum_{k+j=i, 0 \leq k,j} \sigma(k)\tau(j)$$

Example 1.72. *The field of fractions of $\mathbb{F}[[x]]$ is denoted $\mathbb{F}((x))$, which is the formal laurent series denoted:*

$$\mathbb{F}((x)) := \left\{ \sum_{i=N}^{\infty} a_i x^i : N \in \mathbb{Z} \right\}$$

Question 1.73. *Why would we define it in this way?*

If $a_N \neq 0$, then we see

$$A := \sum_{i=N}^{\infty} a_i x^i = x^N \left(\underbrace{a_N + a_{N+1}x^1 + \dots}_{A'} \right) = x^N \sum_{i=N}^{\infty} a_i x^{i-N}$$

Then we see that this becomes a unit in $\mathbb{F}[[x]]$. So A' has an an inverse

$$B' = \sum_{j=0}^{\infty} b_j x^j \in \mathbb{F}[[x]]$$

So we define $B = x^{-N}B'$. It becomes easy to see that $AB = 1$. So to invent $\mathbb{F}[[x]] \setminus \{0\}$ only need x^{-N}. Therefore, $\mathbb{F}((x))$ us a field!

1.5 Chinese Remainder Theorem

See in homework, $R \cong R_1 \times R_2$ corresponds to R having a central idempotent e

$$e \to (1,0)$$
$$1-e \to (0,1)$$

Definition 1.74. *An element $e \in R$ is idempotent provided $e^2 = e$.*

Example 1.75. *In a field, the idempotents are 0 and 1.*

We can think of idempotent elements as projections from the linear algebra sense. The case that $R_j = S/I_j$ has special structure.
Assume all rings below are commutative.

Definition 1.76. *An idempotent e is central if $e \in Z(\mathbb{R})$.*

Definition 1.77. *Two idempotents e, f are orthogonal if $ef = fe = 0$.*

Definition 1.78. *Let $I, J \subset R$ be ideals. I, J are comaximal if $I + J = R$.*

Theorem 1.79. *Let R be a ring with ideals A_i and let*

$$\phi : R \to (R/A_1) \times (R/A_2) \times \ldots \times (R/A_k)$$
$$r \to (r + A_1, r + A_2, \ldots r + A_k)$$

Then

1. *ϕ is a ring homomorphism*
$$Ker(\phi) := \bigcap_{i=1}^{k} A_i$$
2. *Suppose for all $i \neq j$, A_i and A_j are comaximal. Then*
$$A_1 \cap A_2 \cap \ldots \cap A_k = A_1 A_2 \ldots A_k$$
and ϕ is surjective. Hence
$$(R/A_1) \times (R/A_2) \times \ldots \times (R/A_k) \cong R/(A_1 \cap A_2 \cap \ldots \cap A_k) = R/(A_1 A_2 \ldots A_k)$$

Example 1.80. *$R = \mathbb{Z}$ and define $A_i := \langle n_i \rangle := n_i\mathbb{Z}$. Then*

$$\langle n \rangle + \langle m \rangle = 1 \iff gcd(n,m) = 1$$

So in this case, $\langle n \rangle \cap \langle m \rangle = \langle nm \rangle$. The Chinese Remainder Theorem says

$$\mathbb{Z}/(nm\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Warning: If they are not relatively prime! We don't get a surjection!

$$\langle 6 \rangle \cap \langle 15 \rangle = \langle 30 \rangle$$

$$\langle 6 \rangle + \langle 15 \rangle = \langle 3 \rangle$$

Example 1.81. *$R = \mathbb{Q}[x]$ or $\mathbb{F}[x]$,*

$$\mathbb{Q}[x]/\langle x^3 - 8\rangle \cong \mathbb{Q}[x]/\langle x-2\rangle \times \mathbb{Q}[x]/\langle x^2+2x+4\rangle$$

Notice, $x-2$ and x^2+2x+4 are irreducible over $\mathbb{Q}$. However, in $\mathbb{C}[x]$

$$\begin{aligned}\mathbb{Q}[x]/\langle x^3-8\rangle &\cong \mathbb{C}[x]/\langle x-2\rangle \times \mathbb{C}[x]/\langle x^2+2x+4\rangle \\ &\cong \mathbb{C}[x]/\langle x-2\rangle \times \mathbb{C}[x]/\langle x-e^{2\pi i/3}\rangle \times \mathbb{C}[x]/\langle x-e^{2\pi i/4}\rangle \\ &\cong \mathbb{C}\times\mathbb{C}\times\mathbb{C}\end{aligned}$$

Proof. (Of Chinese Remainder Theorem)

1. Seeing that it's a homomorphism is obvious.
2. By induction, it suffices to prove for $k=2$. To see that it's surjective, we see that $1 \in R = A_1 + A_2$ and therefore we can decompose the unit

   $$1 = \underbrace{x}_{\in A_1} + \underbrace{y}_{\in A_2}$$

   Now, given $(r_1 + A_1, r_2 + A_2) \in R/A_1 \times R/A_2$. Let $r = r_1 y + r_2 x$. Then

   $$\begin{aligned}\phi(r) &= (r_1 y + r_2 x + A_1, r_1 y + r_2 x + A_2) \\ &= (r_1(1-x) + r_2 x + A_1, r_1 y + r_2(1-y) + A_2) \\ &= (r_1 + x(r_2 - r_1) + A_1, y(r_1 - r_2) + r_2 + A_2) \\ &= (r_1 + A_1, r_2 + A_2)\end{aligned}$$

   A better way to see this is to notice

   $$\phi(x) = (x + A_1, x + A_2) = (0 + A_1, 1 + A_2)$$
   $$\phi(y) = (y + A_1, y + A_2) = (1 + A_1, 0 + A_2)$$

   So we have found orthogonal idempotents. So we may project to $\langle 0\rangle \times R/A_2$ and $R/A_1 \times \langle 0\rangle$ respectively! Therefore,

   $$\begin{aligned}(r_1 + A_1, r_2 + A_2) &= (r_1(1+A_1), r_2(0+A_2)) + (r_1(0+A_1), r_2(1+A_2)) \\ &= (r_1 + A_1, r_1 + A_2)(1 + A_1, 0 + A_2) + (r_2 + A_1, r_2 + A_2)(0 + A_1, 1 + A_2) \quad = \phi(r_1)\phi(y) + \phi(r_2)\phi \\ &= \phi(r_1 y + r_2 x)\end{aligned}$$

   So with a nod to the First Isomorphism Theorem, we finish the proof!

■

Corollary 1.81.1. *If p_{i_k} are distinct primes with $a_i \geq 1$, and $n = \prod_{i=1}^k p_i^{a_i}$, then*

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^k \mathbb{Z}/p_i^{a_i}\mathbb{Z}$$

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^k (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$$

So

$$\phi(n) = \prod \phi(p_i^{a_i}) = \prod p^{a_i - 1}(p-1)$$

which you may recognize as the Euler Totient Function! That is,

$$\phi(n) = \#\{1 \leq k \leq n : gcd(k,n) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^\times$$

This shows that ϕ is multiplicative!

$$\phi(a,b) = \phi(a)\phi(b) \iff gcd(a,b) = 1$$

2 Domains

2.1 Euclidean Domains

Assume that all rings are commutative in this chapter. Moreover, we can assume they are all integral domains.

Definition 2.1. *Let R be an integral domain. Define $N : R \to \mathbb{N}$ with $N(0) = 0$ to be a norm. Furhter, if $N(a) > 0$ for $a \neq 0$, we call it a positive norm.*

Example 2.2.

$$\begin{aligned} N : \mathbb{Z} &\to \mathbb{N} \\ a &\to |a| \end{aligned}$$

Example 2.3.

$$\begin{aligned} N : \mathbb{F}[x] &\to \mathbb{N} \\ f(x) &\to deg(f(x)) \end{aligned}$$

Definition 2.4. *Let R be an integral domain. R is an Euclidean Domain if it possesses a Division Algorithm with respect to a norm N. That is, for all $a, b \in R, b \neq 0$, there exists $q, r \in R$ such that*

$$a = gb + r$$

with $r = 0$ or $N(r) < N(b)$

Example 2.5. *$R = \mathbb{Z}[i]$ and $N(a + bi) = a^2 + b^2$*

Remark 2.6. *Proving R is NOT a Euclidean Domain is hard.*

Example 2.7. *Let $\mathbb{F}$ be a field. $\mathbb{F}$ is a Euclidean Domain with norm $N(a) = 0$ for all $a \in F$.*

Definition 2.8. *Let R be an integral domain. R is an Principal Ideal Domain (PID) if for any ideal $A \subset R, A = \langle a \rangle$ for some a.*

Example 2.9. *$\mathbb{Z}$ is a PID since all subgroups of $\mathbb{Z}$ and therefore all are singly generated.*

Remark 2.10. *Could have a non-commutative version.*

Remark 2.11. *You could study the idea of a "Principal Ideal Ring", for example $\mathbb{Z}/n\mathbb{Z}$.*

Definition 2.12. *$a, b \in R$ are associates if there exists $u \in R^\times$ such that*

$$b = ua$$

Proposition 2.13. *Let R be an integral domain, and take $a, b \in R$. Then the following statements are equivalent:*

1. *$a|b$ and $b|a$*
2. *$\langle a \rangle = \langle b \rangle$*
3. *a and b are associates.*

Proof. Key Idea: $a|b \iff \langle b \rangle \subset \langle a \rangle$ ■

Example 2.14. *In $\mathbb{Z}$, 5 and -5 are associates.*

Example 2.15. *In $\mathbb{Q}$, $(x - 3)$ and $7(x - 3)$ are associates.*

Example 2.16. *In $\mathbb{F}$, $a, b \neq 0$ are associates.*

Definition 2.17. *Let R be commutative, $b \neq 0, a \in F$, then*

1. *a is a <u>multiple</u> of b if and only if there exists $x \in R$ with $a = bx$*
2. *d is the <u>greatest common divisor</u> $gcd(a, b)$ or a and b if*
   - *$d|a$ and $d|b$*
   - *if $c|a$ and $c|b$ then $c|d$*
3. *L is the <u>least common divisor</u> of a and b if*
   - *$a|L$ and $b|L$*
   - *if $a|M$ and $b|M$ then $L|M$*

Remark 2.18. *Using a norm to measure the greatest common divisor is not needed, nor not really algebraic.*

Remark 2.19. *In a general ring, gcd and lcm need not exist, nor need to be unique, certainly up to associates.*

Recast gcd in the ideal language:

$$d|a \text{ and } d|b \iff \langle a, b\rangle \subset \langle d\rangle$$

Greatest says we cannot sandwich another principal ideal in there. That is, if

$$\langle a, b\rangle \subset \langle c\rangle \subset \langle d\rangle \implies \langle c\rangle = \langle d\rangle$$

Proposition 2.20. *Let R be a PID, with nonzeros $a, b \in R$. Then*

$$\langle a\rangle + \langle b\rangle = \langle a, b\rangle = \langle d\rangle$$

if and only if d is a gcd of a and b. In this case, there exists $x, y \in R$ such that

$$d = ax + by$$

Example 2.21. *In $\mathbb{Z}$, $\langle 30, 7\rangle = \langle 1\rangle$ so we can find*

$$30x + 7y = 1$$

Remark 2.22. *In a Euclicean Domain, the Euclidean Algorithm produces a gcd of a and b.*

$$\begin{aligned}
a &= bq_0 + r_0 \\
b &= r_0q_1 + r_1 \\
r_0 &= r_1q_2 + r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n \\
r_{n-1} &= \underbrace{r_n}_{GCD} q_{n+1} + 0
\end{aligned}$$

Why does this work? If $d|a, d|b \implies d|r_0$. Then in the next step, we get $d|b$ and $d|r_0$. And so on ...

Remark 2.23. *Unraveling produces $x, y \in R$ with*

$$r_n = d = ax + by$$

But we don't need a Euclidean Domain for this, it holds in PIDs.

Proposition 2.24. *If R is a Euclidean Domain, then it is a PID. In fact $A = \langle a\rangle$ for any $a \neq 0$ of minimal norm.*

Proof. Just like in $\mathbb{Z}$, you showed for any subgroup of $(\mathbb{Z}, +)$, was simply $n\mathbb{Z}$. Lastly, use the division algorithm and pick element of smallest norm. ■

Example 2.25. $\mathbb{Z}[\sqrt{-5}]$ *is NOT a PID! You'll see in the homework ,*

$$I_2 = \langle 2, 1+\sqrt{-5}\rangle \quad I_3 = \langle 3, 2+\sqrt{-5}\rangle$$

One idea is, to assume we can write $I = \langle a\rangle \implies 2 = ab \quad 1+\sqrt{-5} = ac$
Think about $z\bar{z} = a\bar{a} = b\bar{b}$ *and we know about the divisibility in* $\mathbb{Z}$.

Example 2.26. $\mathbb{Q}[x]$ *is a PID and a ED!*

Example 2.27. $\mathbb{Z}Z[x]$ *is NOT a PID. Usual,* $I = \langle 2, x\rangle$*, which is pretty easy to show.*

Example 2.28. $\mathbb{Q}[x, y]$ *is NOT a PID. Even farther,* $I = \langle x, y\rangle$.

Exercise 2.29. *Find a PID that is not a ED.*

Definition 2.30. *Let* $\mathbb{F}$ *be a field,* $f(x) \in \mathbb{F}[x], a \in \mathbb{F}$. *a is a* <u>root</u> *of* f *if* $f(a) = 0$.

Proposition 2.31. $a \in \mathbb{F}$ *is a root of* $f(x) \in \mathbb{F}[x]$ *if and only if* $(x-a)|f(x)$ *in* $\mathbb{F}[x]$.

Proof.

- ($\Rightarrow$) if $f(x) = (x-a)g(x)$ then $f(a) = (a-a)g(a) = 0$
- ($\Leftarrow$) Suppose $f(a) = 0$, then

  $$f(x) = (x-a)g(x) + r(x)$$

  with $r(x) = 0$ or $deg(r(x)) < deg(x-a) = 1$. Therefore, r is constant. So

  $$0 = f(a) = (a-a)g(a) + r = r$$

  So $r = 0$.

■

Proposition 2.32. *If* $f(x) \in \mathbb{F}[x]$ *has degree* n*, then* f *has at most* n *roots.*

Definition 2.33. *We say a root* a *has* <u>multiplicity</u> m *if* $(x-a)^m|f(x)$ *but* $(x-a)^{m+1} \nmid f(x)$.

Remark 2.34. *The previous propsition is false when* $K[x]$ *for* K *not a field.*

Example 2.35. $K = \mathbb{Z}/8\mathbb{Z}$*, with* $f(x) = x^2 - 1$*. Then*

$$x^2 - 1 = (x-1)(x+1) = (x-3)(x+3)$$

Theorem 2.36. *Let* $\mathbb{F}$ *be a field.* $G \subset \mathbb{F}^\times$ *a subgroup with* $|G| < \infty$*. Then* G *is cyclic. In particular, if* $|F| < \infty$ *with* $F^\times$ *is cyclic.*

Proof. G is a finite Abelian group. By the structure theorem, we know

$$G = C_{n_1} \times C_{n_2} \times \ldots \times C_d$$

with $n_i|d$. So in particular, $g^d = 1$ for all $g \in G$. $x^d - 1$ has at most d roots in $\mathbb{F}$. So $|G| \leq d$. So we have forced $G \cong C_d$ ■

Proposition 2.37. *Let* R *be an integral domain. Suppose* $p \in R$ *is prime. Then* p *is irreducible.*

Proof. Suppose $p = ab$. In particular, $p|ab$. By definition, $p|a$ or $p|b$. Without loss of generality, $p|a$. We can write $a = pr$. So

$$p = ab = prb$$

R is a domain and we don't count 0 as a prime. By cancellation, we see:

$$1 = rb \in b \in \mathbb{R}^\times$$

Hence, p is irreducible. ■

Remark 2.38. *The converse need not hold! In $R = \mathbb{Z}[\sqrt{-5}]$ then 3 is irreducible but not prime.*

Proposition 2.39. *Let R be a PID, with $p \neq 0, p \notin R^\times$. p is prime if and only if p is irreducible.*

One strategy to prove this would be to notice:

- prime if and only if irreducible holds in UFD
- R is a PID implies R is a UFD

Dummit-Foote doesn't prove it this way unfortunately.

Proof.
- ($\Rightarrow$) is 8.3.10 in DF
- ($\Leftarrow$) Suppose $p|ab$ and p is irreducible. Let $d = gcd(p, a)$. So

$$p \in \langle d \rangle = \langle p \rangle + \langle a \rangle$$

So $p = cd \implies c, d \in R^\times$

  - *Case:* $c \in R^\times \implies \langle p \rangle = \langle d \rangle = \langle p \rangle + \langle a \rangle \implies \langle a \rangle \subset \langle p \rangle \implies p|a$
  - *Case:* $d \in R^\times$. Then there exist r, s with $rp + sa$

$$b = prb + sab \implies p|b$$

■

2.2 Unique Factorization Domains

Definition 2.40. *A unique factorization domain is an integral domain R such that for any $r \in R, r \neq 0, r \notin R^\times$*

1. *Can write $r = p_1 p_2 \dots p_n$ with $n < \infty$, p_i irreducible.*
2. *The above is unique up to permutation and multiplication by associates.*

In the homework, we saw an example that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Proposition 2.41. *Let R be a UFD, $p \neq 0, p \notin R^\times$. Then p is prime if and only if p is irreducible.*

Proof.
- ($\Rightarrow$) 8.3.10
- ($\Leftarrow$) Suppose p is irreducible and $p|ab$. Then

$$a = q_1 \cdot \ldots \cdot q_m \quad b = r_1 \cdot \ldots \cdot r_n$$

and write $ab = pc$. Now, to see that p is an associate to some $q_i \implies p|a$ or p is an associate to some $r_j \implies p|b$.

■

Remark 2.42. *See Proposition 8.3.13 which shows how to construct gcd in the way we learned in school for $\mathbb{Z}$.*

Example 2.43.

$$gcd(18, 81) = gcd(2 \cdot 3^2, 3^3) = 2^0 3^2 = 9$$

Theorem 2.44. *Let R be a PID. Then R is a UFD.*

Proof. Do on your own time.

Basic Idea: Assume a is irreducible. Then keep factoring the element until the process terminates. This termination is guaranteed because PIDs are Noetherian. ■

Fields $\subset$ ED $\subset$ PID $\subset$ UFD $\subset$ Integral Domains

Example 2.45. *The primes in $\mathbb{Z}[i]$, which are given by those $p \equiv 3 \mod 4$. Otherwise, there exists $\pi \in \mathbb{Z}[i]$ such that $\pi\bar{\pi} = p \equiv 1 \mod 4$, or $p = 2$.*

We can identify these primes by looking at the norm:

$$N(a + b\sqrt{D}) = a^2 - Db^2$$

and it has the form p or p^2 for a prime $p \in \mathbb{Z}$.
We can also consider the flipped perspective: Take prime $p \in \mathbb{Z} \implies p \in \mathbb{Z}[\sqrt{D}]$ too. Does it stay prime / irreducible? Sometimes yes, sometimes no.

Proposition 2.46. *Given a homomorphism $\phi : R \to S$ with $Q \subset S$ a prime ideal. Then $\phi^{-1}(Q) \subset R$ is also prime.*

Proposition 2.47. *Let R be a PID with $I \subset R$ is an ideal. Then I is prime if and only if $I = \langle 0 \rangle$ or $I = \langle p \rangle$ for some prime element $p \in R$. In the case that $I = \langle p \rangle$, then I is maximal.*

Proof. Think about if p is irreducible and recall $\langle b \rangle \supset \langle a \rangle \implies b|a$. ■

Proposition 2.48. *Let $I \subset R$ be an ideal. Then*

$$R/I[x] \cong R[x]/\langle I \rangle$$

where $\langle I \rangle \subset R[x]$ is ideal generated by I:

$$\langle I \rangle := \{\sum a_k x^k : a_k \in I\}$$

If $I \subset R$ is prime, then $\langle I \rangle \subset R[x]$ is prime.

Proof. Consider

$$\phi : R[x] \to R/I[x]$$
$$\sum_k a_k x^k \to \sum_k \bar{a}_k x^k$$

with $Ker(\phi) = \langle i \rangle = \phi^{-1}(0)$. Then if $I \subset R$ is, R/I is an integral domain and $\langle 0 \rangle \subset R/I$ is prime. That is, if $R/I[x]$ is an integral domain, then

$$R/I[x] \implies \langle I \rangle \subset R[x] \text{ is prime}$$

■

Remark 2.49. *If you can factor a monic polynomial upstairs, then you can also factor downstairs.*

$$\phi(g(x)h(x)) = \phi(g(x))\phi(h(x))$$

So if irreducible downstairs, then it's also irreducible upstairs.

Theorem 2.50. *Let $\mathbb{F}$ be a field. Then $\mathbb{F}$ is a E.D. Hence, it's a PID and UFD.*

Exercise 2.51. *IF $\mathbb{F}$ is a field, and $f(x) \in \mathbb{F}[x]$ has degree n, then*

$$dim_{\mathbb{F}}(\mathbb{F}[x]/\langle f \rangle) = n$$

In particular, a basis is $\{1, x, x^2, \ldots, x^{n-1}\}$. So if $|\mathbb{F}| = q$, then the size of the this new space is at most q^n.

Question 2.52. *Let R be a UFD with $\mathbb{F}$ the field of fractions. Can we compare $R[x]$ and $\mathbb{F}[x]$?*

Example 2.53. *$\mathbb{Z}[x]$ and $\mathbb{Q}[x]$, which leads us to Gauss's Lemma.*

Example 2.54. $\mathbb{F}[x] \supset \{\sum_{i=0}^{n} a_i x^i : n \in \mathbb{N}, a_1 = 0\}$

Note 2.55. *R is a subring, but not a UFD. Then $x^2, x^3 \in R$ both are irreducible, but not prime.*

$$x^6 = x^2 \cdot x^2 \cdot x^2 = x^3 \cdot x^3$$

Proposition 2.56. *If R is a UFD, so is $R[x]$.*

Example 2.57. *$\mathbb{Z}[x]$ is a UFD, but not a PID. $\mathbb{Z}[x, y]$ is a UFD.*

Lemma 2.58. *Let $c \in \mathbb{F}$. $g(x) \in \mathbb{F}[x]$ is irreducible if $g(x + c) \in \mathbb{F}[x]$ is irreducible.*

Theorem 2.59 (Eisenstein's Criterion)**.** *Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$. Suppose there exists a prime $p \in \mathbb{Z}$ such that*

$$p | a_i, \quad p \not| a_n \quad p^2 \not| a_0$$

Then $f(x) \in \mathbb{Q}[x]$ is irreducible.

Proof. Suppose $f(x) = b(x)c(x)$. We may assume $b(x), c(x) \in \mathbb{Z}[x]$. We can extend $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ to $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ with the mapping $g \to \bar{g}$. Then $\bar{f} = \bar{a}_n x^n \implies \bar{b} = \bar{u}x^m, \bar{c} = \bar{v}x^{n-m}$. So $\bar{u}, \bar{v} \in \mathbb{F}_p^{\times}$. In particular, $\bar{b}_0 = \bar{c}_0 = 0$. So $p | b_0, p | c_0 \implies p^2 | b_0 c_0 = a_0$. ■

Proposition 2.60. *We can generalize to P = prime ideal in R an integral domain. If $a_n = 1$, $a_i \in P$ with $0 \leq i < n$, with $a_0 \notin P^2$.*

Theorem 2.61. *Let $p \in \mathbb{Z}$ be prime. Then*

$$\Phi_p(x) = 1 + x + \ldots + x^{p-1} \in \mathbb{Q}[x]$$

is irreducible.

Proof. Notice $\Phi_p(x) = \frac{x^p - 1}{x - 1}$. Let

$$f(x) = \Phi_p(x + 1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k-1}$$

f satisfies Eisenstein's Criterion so $\Phi_p(x)$ is irreducible. ■

Definition 2.62. *A collection of objects I_α satisfies the ascending chain condition if*

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

eventually stabilizes. That is, there exists N such that for all $i, j > N, I_i = I_j$.

One could also say any strictly ascending chain is finite.

Definition 2.63. *A collection of objects I_α satisfies the descending chain condition if*

$$I_1 \supset I_2 \supset I_3 \subset \ldots$$

eventually stabilizes. That is, there exists N such that for all $i, j > N, I_i = I_j$.

Definition 2.64. *A ring R is noetherian if is satisfies the ascending chain condition on ideals. When in the noncommutative setting, you often stipulating the condition for left ideals.*

Definition 2.65. *A ring R is Artinian if it satisfies the descending chain condition on ideals.*

Example 2.66. *$\mathbb{Z}$ is Noetherian but not Artinian*

$$\langle 6\rangle \subset \langle 3\rangle \subset \langle 1\rangle$$

$$\langle 6\rangle \subset \langle 2\rangle \subset \langle 1\rangle$$

Recall, containment of ideals is equivalent to divisibility in a PID. On the flip side, we can infinitly multiply integers;

$$\ldots \subset \langle 48\rangle \subset \langle 24\rangle \subset \langle 12\rangle \subset \langle 6\rangle$$

Fact: If R is Artinian, then R is Noetherian. **Fact:** If $|R| < \infty$, then R is Noetherian and Artinian.

Proposition 2.67. *The following statements are equivalent:*

1. *R is Noetherian*
2. *Every nonempty family $\mathcal{F}$ of ideals of R has a maximal element. i.e. $\exists \eta \in \mathcal{F}$ such that if $I \in \mathcal{F}$, with $\eta \subset I \implies \eta = I$*
3. *Every ideal of R is finitely generated.*

Corollary 2.67.1. *A PID is Noetherian.*

Proof.

- (1) $\Rightarrow$ (2) : Suppose R is Noetherian. If $I_1 \subset \mathcal{F}$ is not maximal, we pick $I_2 \in \mathcal{F}$ such that $I_1 \subset I_2$. Repeat. By the ascending chain condition, this eventually terminates to the maximal element of $\mathcal{F}$. **Warning:** this maximal element in $\mathcal{F}$ is not necessarily the maximal element of R.
- (2) $\Rightarrow$ (3) : Let $I \subset R$ be any ideal. Let $\mathcal{F} :=$ the family of all finitely generated subideals of I. Since

  $$\langle 0\rangle \subset I \implies \mathcal{F} \neq \emptyset$$

  Now, let $\eta \in \mathcal{F}$ be maximal. So $\eta \subset I$. If η was a proper subset of I, then we pick $a \in I \setminus \eta andconsider$

  $$J = \eta + \langle a\rangle$$

  The J is finitely generated and a subset of I, but $\eta \subset J \neq \eta$. So $J \in \mathcal{F}$ by the maximality of η. So $I = \eta$ is finitely generated.
- (3) $\Rightarrow$ (1) : Let $I_1 \subset I_2 \subset \ldots$ be an ascending chain. Let

  $$J := \bigcup_{k\geq 1} I_k$$

  Then J is an ideal. By the hypothesis in statement (3), J is finitely generated, so we can write

  $$J = \langle a_1, \ldots, a_n\rangle = \langle a_1\rangle + \langle a_2\rangle + \ldots + \langle a_n\rangle$$

  By the definition of the union, for each $1 \leq i \leq n, a_i \in I_{k_i}$. Define $N := \max_{1\leq i\leq k} k_i$. Then for all $a_i \in I_N$, then $J \subset I_N$. Thus the chain stabilizers at N. And R satisfies the ascending chain condition on ideals, and hence Noetherian.

■

Remark 2.68. *Not every ring that satisfies the ascending chain condition on its ideals is Noetherian.*

Example 2.69. *Let $S = \{f : \mathcal{R} \to \mathbb{R}\}$ under pointwise addition and multiplication. Define*

$$I_k := \{f \in S : f(x) = 0 \ \ \forall\ x \geq k\}$$

Then

$$I_1 \subset I_2 \subset \ldots$$

is an ascending chain that never stabilizes. So S is not Noetherian and $J := \bigcup_k I_k$ is not finitely generated.

Corollary 2.69.1. *If R is Noetherian and $I \subset R$ is an ideal. Then there exists a maximal η with*

$$I \subset \eta \subset R$$

In particular, maximal ideals exist.

Theorem 2.70 (Hilbert Basis)**.** *If R is Noetherian, so is $R[x]$*

2.3 The Integral Domain $\mathbb{F}[x]$ when $\mathbb{F}$ is a field

We know $\mathbb{F}[x]$ is an ED, hence PID. So we would want to understand $\mathbb{F}[x]/I$.
A nice parallel is to look at $\mathbb{Z}/I$ where we know $I = \langle n \rangle$. Further, we can factor

$$n = \prod p_i^{e_i}$$

where p_i is prime / irreducible, $p_i \neq p_j$ and $e_i \geq 1$. Then as a consequence of the chinese remainder theorem,

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_i \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

There is no difference for $\mathbb{F}[x]$ with $I = \langle g(x) \rangle$. We can factor

$$g(x) = \prod p_i(x)^{e_i}$$

with $p_i(x)$ prime / irreducible, $e_i \geq 1$. Therefore,

$$\mathbb{F}[x]/\langle g(x) \rangle \cong \prod \mathbb{F}[x]/\langle p_i(x)^{e_i} \rangle$$

Exercise 2.71. *Show $\mathcal{F}[x]/p(x)^e$ is indecomposable. Moreover, if $e = 1$, then it's fill*

3 Modules

Definition 3.1. *Let R be a ring. A left R-module M or ${}_RM$ is an abelian group $(M,+)$ with an action*

$$R \times M \to M$$
$$(r,m) \to r \cdot m$$

such that

1. $(r+s)\cdot m = r\cdot m + s\cdot m$ *for all* $r,s \in R, m \in M$
2. $(rs)\cdot m = r\cdot(s\cdot m)$ *for all* $r,s \in R, m \in M$
3. $r\cdot(m+n)\cdot m = r\cdot m + r\cdot n$ *for all* $r \in R, m,n \in M$
4. $1\cdot m = m$ *for all* $m \in M$

Remark 3.2. *A right R-module M_R is similar with action $M \times R \to M$.*

Remark 3.3. *We can denote the set of R-modules as $R-mod$*

Definition 3.4. $R^{op} :=$ *is the ring with some underlying set R but*

$$r \cdot s = sr$$

An R-module is the same as an mod-R^{op}.

Note 3.5. *In the case that R is commutative, $R \cong R^{op}$.*

Example 3.6. $R = \mathbb{M}_n\mathbb{C}$ *with* $R \cong R^{op}$ *defined with*

$$f : \mathbb{M}_n\mathbb{C} \to (\mathbb{M}_n\mathbb{C})^{op}$$
$$A \to A^T$$

we can check

$$(AB)^T = f(AB) = \underbrace{f(A)\cdot f(B)}_{\text{in } R^{op}} = \underbrace{f(B)f(A)}_{\text{in matrix mult}} = B^TA^T$$

And $f(I_n) = I_n, f(A+B) = f(A)+f(B)$. So if a ring has an anti-automorphism, then $R \cong R^{op}$

Example 3.7. $A \to A^{-1}$ *cannot serve as such an action on $\mathbb{M}_n\mathbb{C}$ since not every $A \in \mathbb{M}_n\mathbb{C}$ is invertible.*

Example 3.8. *Let $\mathbb{F}$ be a field. Then a left $\mathbb{F}M$ or ${}_{\mathbb{F}}M$ is exactly a $\mathbb{F}$-vector space.*

Definition 3.9. *Let R be a ring, $M \in R$-mod. A submodule or R-submodule of M is a subset $N \subset M$ such that $(N,+) \leqslant (M,+)$ is a subgroup and for all $r \in R$, for all $n \in N, r\cdot n \in N$.*

Definition 3.10. *Let $M,N \in R$-mod. An R-module homormorphism $\phi : M \to N$ is a homormophism of abelian groups respecting the R action:*

$$\phi(r\cdot m) = r\cdot\phi(m)$$

for all $m \in M$. Further,

$$Hom_R(M,N) := \text{ all such } R\text{-module homomorphisms}$$

Example 3.11. $R = \mathbb{F}$. *If ${}_{\mathbb{F}}V, {}_{\mathbb{F}}W$, then an $\mathbb{F}$-module homomorphism is exactly a linear transformation / linear map. An $\mathbb{F}$-submodule of V is a subspace (sub vector space).*

Example 3.12. *For a general ring R, the regular left R-module ${}_{\mathbb{R}}R$ is R with and R action $r\cdot s := rs$.*

Question 3.13. *What are the R-submodules?*

R-submodules are exactly the left ideals with $I \subset R$.

Question 3.14. *What are the R-module homomorphisms $\phi : {}_{\mathbb{R}}R \to {}_{\mathbb{R}}R$?*

ϕ is determined by $\phi(1) = s$ for some $s \in {}_{\mathbb{R}}R$. And so:

$$\phi(r) = \phi(r \cdot 1) = r \cdot \phi(1) = r \cdot s = rs$$

Call $\phi = \phi_s$. This is indeed an R-module homomorphism. So
Is this all of them?

$$End_R(R) := Hom_R({}_{\mathbb{R}}R, {}_{\mathbb{R}}R) \cong (R^{op})$$
$$\phi_s \leftarrow s$$

Example 3.15. *$R = \mathbb{Z}$. So, for the $\mathbb{Z}$-module homomorphisms M, we see the $(M, +)$ is a group. So the $\mathbb{Z}$-module homomophisms are the normal abelian groups of $\mathbb{Z}$, which are exactly the subgroups of $\mathbb{Z}$.*

Definition 3.16. *Let k be a commutative ring. A ring A is a $\underline{k\text{-algebra}}$ if we have a ring homomorphism $f : k \to A$ such that $f(k) \subset Z(A)$.*

Remark 3.17. *Notice, we need not be injective.*

Example 3.18. *$\mathbb{Z}/3\mathbb{Z}$ is a $\mathbb{Z}$-algebra but NOT a $\mathbb{Q}$-algebra.*

Remark 3.19. *Often, k is a field.*

Example 3.20. *$A = \mathbb{Q}[x]$ is a $\mathbb{Q}$-algebra.*

Example 3.21. *$B = \mathbb{Z}[x]$ is a $\mathbb{Z}$-algebra.*

Example 3.22. *$C = \mathbb{M}_n(\mathbb{C})$ is a $\mathbb{C}$-algebra where*

$$f : \mathbb{C} \to \mathbb{M}_n(\mathbb{C})$$
$$a \to aI_n$$

Example 3.23. *Any ring R is a $\mathbb{Z}$-algebra, with*

$$\mathbb{Z} \to R$$
$$n \to \underbrace{1 + 1 + \ldots + 1}_{n}$$

Example 3.24. *Let $k = \mathbb{Q}$ with $G = D_n$ the dihedral group. Then*

$$k[G] = \mathbb{Q}[D_n]$$

us the group algebra, and is a $\mathbb{Q}$-algebra. Underlying set is the $\mathbb{Q}$ vector space with basis $g \in G$. Recall

$$D_n = \{e, x, x^2, \ldots, x^{n-1}, y, xy, x^2y, \ldots, x^{n-1}y\}$$

So

$$\implies \frac{2}{3}x - 17xy + \frac{1}{4}e \in \mathbb{Q}[D_n]$$

multiplication comes from D_n and distributivity. So

$$f : \mathbb{Q} \to \mathbb{Q}[D_n]$$
$$a \to ae$$

realizes the $\mathbb{Q}$-algebra structure.

Example 3.25. *If R is a ring with subring $S \subset R$, and ${}_{\mathbb{R}}M$, then M is also a left S-modules.*

3.1 $\mathbb{F}[x]$-modules

Let V be a $\mathbb{F}[x]$-module. By restriction, V is also an $\mathbb{F}$-module. Since $\mathbb{F}$ is a field, then V is an $\mathbb{F}$-vector space.

Question 3.26. *What about x?*

$x : V \to V$ is a $\mathbb{F}$-linear map. We can check this

$$x \cdot (\alpha v + \beta w) = x \cdot (\alpha v) + x \cdot (\beta w) = \alpha x(v) + \beta x(w)$$

So x can be thought of as a linear map. Further $\mathbb{F}[x]$-modules can be thought of identically as $\mathbb{F}$-vector spaces V with a distributed linear map $T : V \to V$.
Now that we have this characterization, what can be said about the homomorphisms between two $\mathbb{F}[x]$-modules V and W:

$$Hom_{\mathbb{F}[x]}(V, W)$$

Let $f \in Hom_{\mathbb{F}[x]}(V, W)$. Then $f : V \to W$ is a linear map. Moreover, to be a module homomorphism, we need to satisfy

$$f(x \cdot v) = x \cdot f(v)$$
$$f(T(v)) = S \cdot f(v)$$

So we need this diagram to commute.

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle S} \\ V & \xrightarrow{f} & W \end{array}$$

So if f is an isomorphism of $\mathbb{F}[x]$-modules, then $T = f^{-1}Sf$. This should be recognized as the change of bases formula.

Observation 3.27. *Let $M \in R$-modules. Then*

$$End_R(M) = Hom_R(M, M) = Hom_R({}_{\mathbb{R}}M, {}_{\mathbb{R}}M)$$

is a ring under composition and pointwise addition

$$(f + g)(r) = f(r) + g(r)$$
$$(f \circ g)(r) = f(g(r))$$

If R is a k-algebra, so is $End_R(M)$.

Example 3.28. *$R = \mathbb{F}, M = V \cong \mathbb{F}^n$. Then*

$$End_{\mathbb{F}}(V) = End_{\mathbb{F}}(\mathbb{F}^n) \cong \mathbb{M}_n(\mathbb{F})$$

3.2 Quotient Modules

Definition 3.29. *Let $M \subset R$-module and $N \subset M$ be an R-submodule. Then M/N is an R-module, so we call a quotient module*

$$r \cdot (m + N) = r \cdot m + N$$

Exercise 3.30. *Prove the quotient module is well-defined.*

Example 3.31. *The natural projection map*

$$\pi : M \to M/N$$
$$m \to m + N$$

is an R-module homomorphism with kernel N. Recall, if $f \in Hom_R(M, M')$, we recall $Ker(f) := \{m \in M : f(m) = 0\}$

Definition 3.32. *Let $M \in R$-module and let A, B be submodules. Then*

$$A + B = \{a + b : a \in A, b \in B\}$$

is an R-submodule. We can extend tho finite sums of submodules as well.

3.3 Isomorphism Theorems

For the setup, let R be a ring, M, N be R-modules, and $A, R \subset M$-submodules.

Theorem 3.33 (First)**.** *Let $\phi \in Hom_R(M,N)$. Then $M/Ker\phi \cong Im(\phi)$*

Theorem 3.34 (Second)**.**

$$(A+B)/B \cong A/A \cap B$$

Theorem 3.35 (Third)**.**

$$A \subset B \subset M \implies (M/A)/(B/A) \cong M/B$$

Theorem 3.36 (Correspondence)**.** *We have a one-to-one correspondence where*

$$\{B such\ that\ A \subset B \subset M\} \leftrightarrow \{submodules\ of\ M/A\}$$

under the mapping

$$B \to B/A$$
$$\pi^{-1}(N) \to N \subset M/A$$

This correspondence is inclusion preserving and commutes with sums and intersections.

Proof. On your own time. ■

Proposition 3.37. *If $\phi : M \to N$ is an R-module homomorphism, and $Ker(\phi)$ and $Im(\phi)$ are R-submodules of M and N respectively.*

Corollary 3.37.1. *Submodules of ${}_RR$ are exactly the left ideals of R.*

3.4 Simple Modules

Definition 3.38. *Let M be an R-module. Then M is <u>cyclic</u> if there exists $a \in M$ such that*

$$M = R \cdot a = \{r \cdot a : r \in R\}$$

Definition 3.39. *Let M be an R-module. $A \subset M$ some subset. Then M is <u>generated by A</u> if*

$$M = RA = \left\{ \sum_{i=1}^{k} r_i a_i : r_i \in R, a_i \in A, k \in \mathbb{N} \right\} (= \{0\}\ if\ A = \emptyset)$$

If there exists an A such that $|A| < \infty$, we say M is finitely generated.

Definition 3.40. ${}_{\mathbb{R}}M$ *is <u>simple</u> (or <u>irreducible</u>) if ${}_{\mathbb{R}}M \neq \{0\}$ and for any R-submodule*

$$0 \subset N \subset M \implies N = \{0\}\ or\ N = M$$

Example 3.41. *Let $R = \mathbb{F}$. Then ${}_{\mathbb{R}}M =$ vector space $= \mathbb{F}^n$. Is $\mathbb{F}^n$ cyclic? In order to force it to be cyclic, we see that we must restrict*

$$dim_{\mathbb{F}}(\mathbb{F}v) = 1 \implies n \leq 1$$

Also, $\mathbb{F}^n$ is finitely generated if $n < \infty$. Also, the Simple $\mathbb{F}$-modules are the 1-dimensional $\mathbb{F}$-vector spaces.

Proposition 3.42. *1. Let ${}_RM$ be cyclic. Then ${}_RM \cong R/I$ for some (left) ideal $I \subset R$.*

2. Let ${}_RM$ be simple. Then ${}_RM \cong R/I$ for some maximal left ideal I.

3. If ${}_RM$ is simple, then it is cyclic. That is, $M = Ra$ for any $0 \neq a \in M$.

Proof. 1. Suppose $M = Ra$. Let

$$\begin{aligned} \phi : R &\to M \\ r &\to r \cdot a \end{aligned}$$

Then ϕ is an R-module homomorphism since

$$\phi(s \cdot r) = \phi(sr) = sr \cdot a = s \cdot (r \cdot a) = s \cdot \phi(r)$$

$$\phi(r_1 + r_2) = (r_1 + r_2) \cdot a = r_1 \cdot a + r_2 \cdot a = \phi(r_1) + \phi(r_2)$$

Then, letting $I = Ker(\phi)$ and $M = Im(\phi)$, then we can invoke the first isomorphism theorem.

2. Use the correspondence theorem.

3. We simply show that Ra is a nonzero submodule. Therefore, $Ra = M$ by the simplicity of M.

■

Example 3.43. *Suppose $R = \mathbb{F}$. Then the nonzero cyclic modules are all the simple simple submodules.*

Example 3.44. *Suppose $R = \mathbb{Z}$. We remember the cyclic modules are isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Note, $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ might not look cyclic but it is as a module. Further, we know it is simple when $n = p$ prime. Recall, groups of prime order are only groups without nontrivial proper subgroups.*

Note 3.45. *In general, the $\mathbb{Z}$-modules are any abelian group.*

Example 3.46. *An example of a $\mathbb{Z}$-modules that is not cyclic is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ generated by $A = \{(0,1),(1,0)\}$.*

Example 3.47. *${}_{\mathbb{Z}}\mathbb{Q}$ is not finitely generated.*

Example 3.48. *${}_{\mathbb{Z}}\mathbb{R}$ is not finitely generated. In this case, use the cardinality argument.*

Example 3.49. *When $R = \mathbb{F}[x]$, a cyclic module will come of the form $\mathbb{F}[x]/\langle f \rangle$.*

Example 3.50. *Let $\mathbb{F} = \mathbb{R}$ with $f(x) = x^4 + 2$, then define*

$$V = \mathbb{R}[x]/\langle x^4 + 2 \rangle$$

Describe as a vector space $V = \mathbb{F}^n$ and what linear transformation corresponds to x?
First, V is an $\mathbb{R}$-vector space of dimension 4. What linear transformation corresponds to x?

$$\begin{aligned} T : V &\to V \\ g(x) &\to xg(x) \end{aligned}$$

Further, any linear transformation of a vector space that has a basis is expressible as a matrix.
Well, we can simply look at how x affects the basis:

$$1 \to x$$

$$x \to x^2$$

$$x^2 \to x^3$$

$$x^3 \to -2$$

Therefore, in the basis $\{1, x, x^2, x^3\}$, then the matrix A of the transformation T is

$$M(T) = A = \begin{pmatrix} 0 & 0 & 0 & -2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Example 3.51. *When $R = \mathbb{F}[x]$, the simple module will come of the form $\mathbb{F}[x]/\langle f\rangle$ provided $\langle f\rangle$ is maximal if and only if f is irreducible.*

Example 3.52. *When $R = \mathbb{F}[x]$, the submodules are of the form $\langle f\rangle$.*

Example 3.53. *$R = \mathbb{M}_5(\mathbb{C})$ with $M = \mathbb{C}^5$. Then ${}_RM$ is simple.*
Claim: *If $v \neq 0$ in $\mathbb{C}^5$, then for any $w \in \mathbb{C}^5$, we can identify a matrix $A \in \mathbb{M}_5(\mathbb{C})$ such that $w = Av$.*

Lemma 3.54 (Schur)**.** *Let R be a ring. ${}_RS$, ${}_RT$ be simple left R-modules, ${}_RM$ be any R-module.*

1. *Let $f \in Hom_R(S, M)$. Then $f \equiv 0$ or f is injective.*
2. *Let $f \in Hom_R(M, S)$. Then $f \equiv 0$ or f is surjective.*
3. *Let $f \in Hom_R(S, T)$. Then $f \equiv 0$ or f is an isomorphism.*
4. *$End_R(S)$ is a division ring. Further, if R is a k-algebra, then $End_R(S)$ is also a k-algebra.*

Proof. 1. If S is simple, then it has no proper nontrivial submodules. Now, let f be a homomorphism between S and M. Further, the kernal $Ker(f) \subset S$ is a submodule. But then $Ker(f) = \{0\}$ or $Ker(f) = S$. If $Ker(f) = \{0\}$, then f is surjective. If $Ker(f) = S$, then $f \equiv 0$.

2. By the same reason, $Im(f) \subset S$. Since S is simple, then $Im(S) = S$ or $Im(S) = \{0\}$. If $Im(S) = S$, then f is surjective. If $Im(S) = \{0\}$, then $f \equiv 0$.

3. Use the previous two claims.

4. **Exercise**

■

Example 3.55. *Let $R = \mathbb{M}_5(\mathbb{C})$ with $S = \mathbb{C}^5$. Then how do we find $End_{\mathbb{M}_5(\mathbb{C})}(\mathbb{C}^5)$? Since $Z(R) = \{aI_n : a \in \mathbb{C}\}$, we see that*

$$End_{\mathbb{M}_5(\mathbb{C})}(\mathbb{C}^5) \cong \mathbb{C}$$

Example 3.56. *Let $R = \mathbb{F}[x]$ with $M = \mathbb{F}[x]/\langle f\rangle$.*

3.5 Bimodules

Definition 3.57. *Let R, S be rings. Let M (or ${}_RM_S$) is an (R, S)-bimodule if*

- *${}_RM$ is a left R-module*
- *M_S is a right S-module*

and for all $r \in R, s \in S, m \in M$,

$$(r \cdot m) \cdot s = r \cdot (m \cdot s)$$

Example 3.58. *If R is a commutative ring, any ${}_RM$ is also a (R, R)-bimodule with $m \cdot s = s \cdot m$.*

Example 3.59. *Let $R = \mathbb{M}_3(\mathbb{C}), S = \mathbb{M}_2(\mathbb{C})$. Let M be the module of 3×2 matrices. Then M is an (R, S)-bimodule. Also, M is a $(R, \mathbb{C})$-bimodule.*

Example 3.60. *For any ring R, any ${}_RM_R$ is also a (R, R)-bimodule. The submodules are comprised of the 2-sided ideals of R.*

Example 3.61. *Given ${}_RM$, let $S = End_R(M)$. We can define ${}_SM$ with $\phi \cdot m = \phi(m)$. Therefore, turn it into $M_{S^{op}}$. Therefore, we can form*

$${}_RM_{S^{op}}$$

with the action

$$r \cdot \phi(m) = r \cdot m \cdot_{op} \phi = \phi(r \cdot m)$$

Proposition 3.62. *$Hom_R({}_RM_S, {}_RN_T)$ is an (S,T)-bimodule.*

In this case, the right T-action is inherited from N, so

$$(\phi \cdot t)(m) = \phi(m) \cdot t$$

the left S-action is inherited from M, so

$$(s \cdot \phi)(m) = \phi(m \cdot s)$$

Example 3.63. *If R is commutative, then $Hom_R({}_RM, {}_RN)$ is an R-module too.*

3.6 Direct Sums and Products via Universal Properties

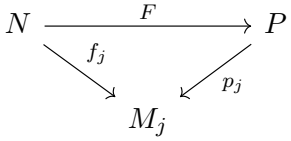
Definition 3.64. *P is a direct product of $\{M_j : j \in I\}$ we are equipped with projection maps*

$$P \xrightarrow{P_j} M_j$$

with the universal property that if any other object N has $N \xrightarrow{f_j} M_j$ for all $j \in I$, then there exists exactly one $F : N \to P$ with

$$p_j \circ F = f_j$$

for all $j \in I$. In particular, the following diagram commutes



Example 3.65. *Let $I = \{1, 2\}$. Then $P = M_1 \times M_2 = \{(m_1, m_2) : m_i \in M_i\}$ with action*

$$r \cdot (m_1, m_2) = (r \cdot m_1, r \cdot m_2)$$

as well as the projections $p_i(m_1, m_2) = m_i \in M_i$. In this case,
Now, suppose $N \xrightarrow{f_1} M_1$ and $N \xrightarrow{f_2} M_2$. Then to make the diagram commute, we see:

$$F(n) = (f_1(n), f_2(n))$$

Exercise 3.66. *Show that p_j are surjective simply as a result of the universal property.*

For rignts or modules or groupes, we can take the Cartesian product

$$P = \prod_{j \in I} M_j = \{(m_j)_{j \in I}\}$$

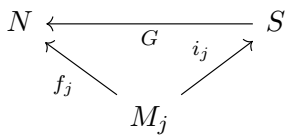
Then each projection becomes:

$$(m_1, m_2, \ldots, m_j, \ldots) \xrightarrow{p_j} m_j$$

Definition 3.67. *S is a coproduct (or direct sum if a module) if we have "inclusions" $M_j \xrightarrow{i_j} S$ such that given any N with maps $M_j \xrightarrow{f_j} N$, there exists a unique map G $S \xrightarrow{G} N$ such that*

$$G \circ i_j = f_j$$

for all $j \in I$. In particular, the following diagram commutes



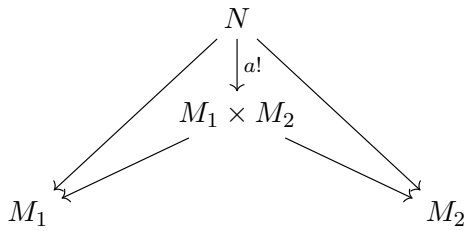
Further, we write

$$S = \bigoplus_{j \in I} M_j$$

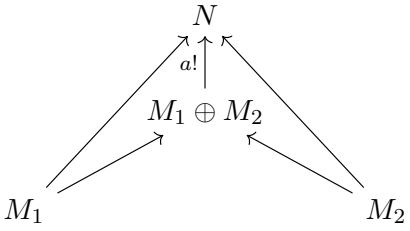
Remark 3.68. *For modules, we can view $\bigoplus_{j\in I} M_j \subset \prod_{j\in I} M_j$ as a submodule with "finite support". That is, all but finitely many entries are 0.*

$$M_k \xrightarrow{i_k} \bigoplus_{j\in I} M_j \subset \prod_{j\in I} M_j$$
$$m \to (0, 0, \ldots, m, 0, \ldots)$$

Example 3.69. *In the case, $|I| = 2$*



Direct Product



Coproduct

So we might intuit

$$M_1 \times M_2 \cong M_1 \oplus M_2$$

Question 3.70. *How would we prove $M_1 \times M_2 \cong M_1 \oplus M_2$ or for any finite $|$?*

- Method 1: Show any such P is isomorphic to $M_1 \times M_2$. Unfortunately, this doesn't work so well.
- Method 2: Show $M_1 \times M_2$ satisfies the universal property of P .

Proof. (Existence) Consider the set of projections:

$$p_i^* : M_1 \times M_2 \to M_i$$
$$(m_1, m_2) \to m_i$$

as well as the given set of R-module homomorphisms $f_j : N \to M_j$. Then we can define the function

$$F : N \to M_1 \times M_2$$
$$n \to (f_1(n), f_2(n))$$

- Check p_i, F are R-module homomorphisms
- Check $p_i \circ F = f_i$:
$$p_i \circ F(n) = p_i(f_1(n), f_2(n)) = f_i(n)$$

These together show that such an F exists.

(Uniqueness) Suppose such another function G exists such that $p_i \circ G = f_i$. Then

$$m_i = p_i((m_1, m_2)) = p_i(G(n)) = f_i(n) \implies m_i = f(n)$$
$$\implies G(n) = (f_1(n), f_2(n)) = F(n)$$

■

Theorem 3.71. *Any two products are isomorphic.*

Proof. Given P with p_i maps, and P' with p_i' maps. So then there exist the unique maps:

$$F : P' \to P$$
$$p_i \circ f \to p_i'$$

$$F' : P \to P'$$
$$p_i' \circ f \to p_i$$

Then, consider $F \circ F' : P \to P$ and so

$$\underbrace{p_j \circ (F \circ F')}_{f_j} : P \to M_j$$

So we end up with a new N such that

$$\tilde{F} : N \to P \quad \text{which satisfies} \quad p_i \circ (F \circ F') = p_i \circ \tilde{F}$$

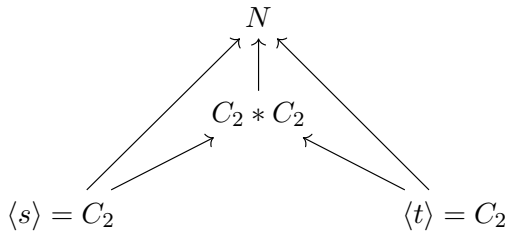
But $id : P \to P$ also works, and since $\tilde{F}$ is unique, then $F \circ F' = id_P$. Similarly, $F' \circ F = id_{P'}$. Therefore, $P \cong P'$. ■

Remark 3.72. *We can check similarly that direct sum $\bigoplus M_i$ are also isomorphic to one another by leveraging the universal property.*

Corollary 3.72.1. *For any finite I, $\bigoplus_{j\in I} M_j = \prod_{j\in I} M_j$*

Remark 3.73. *Abelian groups are $\mathbb{Z}$-modules. For (nonabelian) groups, the coproduct is quite different:*

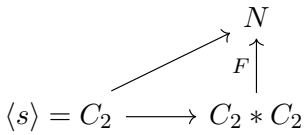
Example 3.74. *We want the following diagram to commute.*



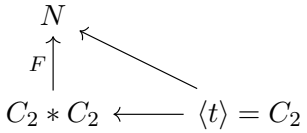
Recall,

$$D_n = \langle x, y | x^n = y^2 = e, yxy^{-1} = x^{-1} \rangle = \langle s, t | s^2 = t^2 = e, \underbrace{stst\dots}_{n} = \underbrace{tsts\dots}_{n} \rangle$$

So we need surjections $C_2 * C_2 \to D_n$ for all n since all the inner diagrams must themselves commute.



So $\langle s \rangle \subset Im(F)$.



So $\langle t \rangle \subset Im(F)$. So $D_n \subset Im(F)$.

Definition 3.75. *Let M be an R-module with submodules $N_i \subset M$ such that*

1. $N_1 + N_2 + \ldots + N_k = M$
2. $i \neq j \implies N_i \cap N_j = \{0\}$

Then $M \cong N_1 \oplus N_2 \oplus \ldots \oplus N_k$, the internal direct product.

Remark 3.76. *This is equivalent to saying for any $x \in M$, there exists a unique expression*

$$x = x_1 + x_2 + \ldots + x_k$$

with $x_i \in N_i$.

Theorem 3.77. *Let R be a ring, with A, B, A_j, B_i as R-modules.*

1. $Hom_R(A, \prod_i B_i) \cong \prod_i Hom_R(A, B_i)$
2. $Hom_R(\oplus_j A_j, B) \cong \prod_j Hom_R(A_j, B)$
3. $Hom_R(A, B_1 \oplus B_2) \cong Hom_R(A, B_1) \oplus Hom_R(A, B_2)$ *and* $Hom_R(A_1 \oplus A_2, B) \cong Hom_R(A_1, B) \oplus Hom_R(A_2, B)$

Remark 3.78. *These are all isomorphisms of $\mathbb{Z}$-modules. In case of appropriate R-mod-S and R-mod-T structures will be S-mod-T isomorphisms.*

Proof. 1. $f \to p_j \circ f$

2. $g \to g \circ i_j$

■

Example 3.79.

$$Hom_{\mathbb{Z}}(\oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \cong \prod Hom_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \cong \prod \mathbb{Z}/2\mathbb{Z}$$

Example 3.80. *Letting $R = \mathbb{F}_2$, then*

$$Hom_{\mathbb{F}}(\oplus_{i \in I} \mathbb{F}, \mathbb{F}) = \prod_{i \in I} Hom_{\mathbb{F}}(\mathbb{F}, \mathbb{F}) = \prod_{i \in I} \mathbb{F}$$

Lemma 3.81. *Given ${}_RM$ and $I \subset R$ is a 2-sided ideal. If $IM = \{0\}$ then M is also an R/I-module.*

Example 3.82. *$\mathbb{Z}/2\mathbb{Z}$ is a $\mathbb{Z}$-modules, but also a $\mathbb{Z}/2\mathbb{Z}$-module and also a $\mathbb{Z}/10\mathbb{Z}$-module.*

Observation 3.83. *An R/I-module M can be thought of as an R-module which satisfies $IM = \{0\}$*

Remark 3.84. *This can serve as a nice trick, in that it sometimes lets us move from $\mathbb{Z}$-modules to $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$-modules. That is, in a commutative ring, it sometimes easy to pass to R/M-modules with M maximal.*

3.7 Free Modules

Definition 3.85. *Let R be a ring and A be a set. The free module $F(A)$ on the set A is the R-module satisfying the universal property:*
We have an inclusion map $A \xrightarrow{i} F(A)$ (not necessarily a homomorphism) such that, given ${}_RM$ which has a map of set $\phi : A \to M$, then there exists a unique R-module homomorphism $\Phi : F(A) \to M$ such that the diagram:

$$\begin{array}{ccc} A & \xrightarrow{\ i\ } & F(A) \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \Phi} \\ & & M \end{array}$$

commutes. Moreover, for every $a \in A$,

$$\phi(a) = \Phi(a) = \Phi(i(a))$$

Theorem 3.86. *If $|A| = n$ with $A = \{a_1, \ldots, a_n\}$, then*

$$\bigoplus_{i=1}^{n} Ra_i = F(A) \cong R^n = \prod_A R$$

We call A a <u>basis</u> of $F(A)$.

Example 3.87. *Consider $F(\{a\}) = Ra$. Since $ra = 0 \implies r = 0$.*

$$\begin{array}{ccc} \{a\} & \xrightarrow{\ i\ } & F(\{A\}) \\ & \searrow^{\phi} & \downarrow \exists! \Phi \\ & & R \end{array}$$

So $\phi(a) = 1 \implies r \cdot 1 = 0 \implies r = 0$. So

$$\Phi(ra) = r\Phi(a) = r \cdot 1 = r$$

Then we see immediately that $Ra \cong R$.

Example 3.88. *$R = \mathbb{Z}$. Then we claim $\mathbb{Z}$ is a free $\mathbb{Z}$-module.*

- *Attempt #1: What if we make $A = \{2\}$ the basis. Then*

  $$2 \to 2 \text{ inclusion}$$

  Then we would need the diagram to commute:

  $$\begin{array}{ccc} \{2\} & \xrightarrow{\ i\ } & \mathbb{Z} \\ & \searrow^{\phi} & \downarrow \exists!? \\ & & \mathbb{Z} \end{array}$$

  However, we cannot send

  $$\begin{aligned} \Phi : \mathbb{Z} &\to \mathbb{Z} \\ 2 &\to 1 \end{aligned}$$

  A concrete way to see that $\{2\}$ fails is to notice the fact that the set $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\} \neq \mathbb{Z}$.

- *Attempt #2: What if we make $A = \{-1, 1\}$ the basis. Then*

  $$\begin{array}{ccc} \{-1,1\} & \xrightarrow{\ i\ } & \mathbb{Z} \\ & \searrow^{\phi} & \downarrow \exists! \Phi \\ & & \mathbb{Z} \end{array}$$

  No such $\mathbb{Z}$-module homomorphism exists. This is because $\{1, -1\}$ fail to be linearly independent since there exists $n, m \in \mathbb{Z}$ such that $n(1) + m(-1) = 0$.

Remark 3.89. *Dummit and Foote define free modules by the existence of a basis, which is the set A.*

Definition 3.90. *A <u>basis</u> of an R-module F is a subset $A \subset F$ such that for all $x \in F \setminus \{0\}$ such that there exists a unique expression*

$$x = r_1 a_1 + r_2 a_2 + \ldots + r_n a_n$$

with $r_i \in R \setminus \{0\}$, $a_i \in A, n \in \mathbb{Z}_{>0}$. If a basis exists, we say F is <u>free on the set A.</u>

Symbolically, we would write

$$F \cong \bigoplus_A R = \bigoplus_{a \in A} Ra$$

Definition 3.91. *When R is commutative, the cardinality of A is called the rank of F.*

Example 3.92. *In $\mathbb{F}$-module V with basis $\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$, then we see that linear independence is*

$$\sum_{i=1}^{n} r_i b_i = 0 \implies r_i = 0 \quad \forall i$$

So if $\sum_{i=1}^n r_i b_i = \sum_{j=1}^n s_j b_j \implies r_i = s_i \implies$ uniqueness of representation.

Example 3.93. *Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/4\mathbb{Z}$. Then ${}_RM$ is not a free module.*

- *Method #1: $M \ncong \mathbb{Z}^{\oplus}$ by counting $4 \neq 0, 4 \neq \infty$*
- *Method #2: There cannot exist a basis. Otherwise, consider $\{\bar{1}\}$. Then for any $x \in \mathbb{Z}/4\mathbb{Z}$ we see that $x = n \cdot \bar{1}$ for some $n \in \mathbb{Z}$. However, $x = (4+n)\bar{1}$, which fails our uniqueness requirement. Alternatively, $0 = 0 \cdot \bar{1} = 4 \cdot \bar{1}$. Any $A \subset \mathbb{Z}/4\mathbb{Z}$ fails.*

Note 3.94. *Warning: One element sets are not classified as linearly independent within modules, as opposed to their vector space counter-parts.*

Example 3.95. *$R = \mathbb{Z}/4\mathbb{Z}$ with $M = \mathbb{Z}/4\mathbb{Z}$ is free with potential bases $A = \{\bar{1}\}$ and $B = \{\bar{3}\}$.*

Example 3.96. *$R = \mathbb{Z}/4\mathbb{Z}$ with $N = \{\bar{0}, \bar{2}\}$ is not free since $\bar{2} \cdot \bar{2} = \bar{0}$, so no basis can be realized.*

Example 3.97. *$R = \mathbb{Z}$ with $M = \mathbb{Q}$ is not free because linear independence fails.*

Example 3.98. *Then $\langle 2 \rangle = 2\mathbb{Z} \subset \mathbb{Z}$ is a free $\mathbb{Z}$-module with $A = \{2\}$ or $B = \{-2\}$.*

Example 3.99. *Then $\langle x^3 + 2 \rangle \subset \mathbb{Q}[x]$ is a free $\mathbb{Q}[x]$-module with $A = \{\frac{7}{3}x^3 + \frac{14}{3}\}$. To see this, check the mapping*

$$\begin{aligned} \mathbb{Q}[x] &\to \langle x^3 + 2 \rangle \\ f &\to f * (x^3 + 2) \end{aligned}$$

is a $\mathbb{Q}[x]$-module isomorphism. To see this, notice,

$$Im\ \phi = \langle x^3 + 2 \rangle \qquad Ker\ \phi = 0$$

We also see that this mapping should be an R-modules homomorphism since it's of the form $r \to rm$ for some $m \in M$.

Question 3.100. *How do I check if ${}_RF$ is free? 3 Methods to try:*

1. *Universal Property*
2. *Does F have a basis?*
3. *$F \cong \oplus\, {}_RR = \oplus_{a \in A} R$*

Example 3.101. *Let $R = \mathbb{Z}$ with $M = 48\mathbb{Z}$. Then ${}_RM$ is a free $\mathbb{Z}$-module since, by (2), we see that $\{48\}$ is a basis, or by (3), we see that $48\mathbb{Z} \cong \mathbb{Z}$ as a $\mathbb{Z}$-module isomorphism with*

$$\begin{aligned} \phi : \mathbb{Z} &\to 48\mathbb{Z} \\ n &\to n \cdot 48 \end{aligned}$$

Example 3.102. *The same proof in the previous examples works for $R = \mathbb{C}[x]$ with $M = \langle x^3 + 2 \rangle = \langle x^3 + 2 \rangle \mathbb{C}[x]$.*

Remark 3.103. *Is a finitely generated submodule of a free module also a free module? Not necessarily. It is guaranteed when the original submodule is a PID.*

Example 3.104. *Let $R = \mathbb{Z} \times \mathbb{Z}$ and define $N = L = \mathbb{Z}$. Define the action*

$$(a, b) \cdot n = na$$

$$(a, b) \cdot l = bl$$

It's not immediately obvious that these actions are valid. To check, we see for the first one

$$(a, b) \cdot (cn) = (a, b)((c, d) \cdot n) = acn = ((ac, bd)) \cdot n = ((a, b)(c, d)) \cdot n$$

$$((a, b) + (c, d)) \cdot n = (a + c)n = (a + c, b + d) \cdot n$$

Note 3.105. *It's not enough for me to give you the set. I must also give you the action.*

Now, we see $N \cong \{(n, 0)\} \subset \mathbb{Z} \times \mathbb{Z}$, which is a finitely generated submodule. Certainly N is generated by $(1, 0)$ as a $\mathbb{Z} \times \mathbb{Z}$ -module. However, N is NOT free. Otherwise, let's try and find a basis for N.

- *Our first candidate for a basis is $\{1\} \subset N$. Clearly it's spanning since for any $n \in \mathbb{Z}$,*

  $$(n, 0) \cdot 1 = (n, 0) \cdot (1, 0) = n$$

  But we see we lack independence

  $$(n, 3) \cdot 1 = n$$

- *Since $N \neq \{0\}$, then the basis $\mathcal{B}$ is nonempty. Letting $b \in \mathcal{B}$, we see that*

  $$(n, 0) \cdot b = (n, 3) \cdot b$$

  and therefore we always violate uniqueness.

"When rings are not domains, lots of weird stuff can happen." - Vazirani quote of the day.

Question 3.106. *If M is free, the is annihilator of m zero for every $m \in M$? No! This is true for every element in your basis.*

Example 3.107. *Let $R = \mathbb{Z} \times \mathbb{Z}$. Then $M = {}_R R$ is free with basis $\mathcal{B} = \{(1, 1) = id_R\}$. Moreover, we can use any unit $u \in R^\times$ as a basis. Now, let $m = (1, 0)$. Then*

$$Ann_R(m) = \{(a, b) : (a, b)(1, 0) = (0, 0)\} = \{(b, 0)\} \neq \{0\}$$

Theorem 3.108. *The following statements about free modules are equivalent:*

1. *Universal Property*
2. *Does F have a basis?*
3. *$F \cong \oplus\, {}_R R = \oplus_{a \in A} R$*

Proof.

- (2) $\implies$ (3) : If A is a basis of F, then define the mapping

  $$\oplus_{a \in A} R \to F$$
  $$(r_a, r_b, r_c, \ldots) \to \sum_{a \in A} r_a a$$

  Notice the right hand side is finite since all but finitely many r_a is zero. Further, ϕ is surjective since A "spans" F and by the linear independence of our basis, we must have uniqueness, and therefore injectivity. Therefore, we have an isomorphism.

- (3) $\implies$ (2) : The reverse direction is simply writing each a as the standard basis.

Relating (1) to these statements is summarized in the next proposition. ■

Proposition 3.109. $F(A) \cong \bigoplus_{a\in A} Ra$

Proof. Suppose I have a free module $F(A)$. By the universal property, we know there exists Φ

$$\begin{array}{ccc} A & \xrightarrow{\ i\ } & F(A) \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists!\Phi} \\ & & \bigoplus_{a\in A} Ra \end{array}$$

Fill-In ■

Proof. (3) $\iff$ (1) (Alternative)
We can show that $\bigoplus_{a\in A} Ra \cong \bigoplus_{a\in A\ R} R$ using the universal property. Define

$$\begin{aligned} i : A &\to \oplus Ra \\ a &\to (0, 0, \ldots, 0, a, 0, 0, \ldots) \end{aligned}$$

with a in the a coordinate. Notice $\oplus Ra \subset \prod Ra$. Now, suppose we are given

$$\phi : A \to {}_R M$$

Now, we want to define a Φ such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{\ i\ } & \bigoplus_{a\in A} Ra \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists!\Phi} \\ & & M \end{array}$$

commutes. Define

$$\Phi(0, 0, \ldots, 0, a, 0, 0, \ldots) = \phi(a)$$

This determines Φ as any $x \in \bigoplus_{a\in A} Ra$ and can be written as the finite sum

$$x = \sum_a r_a \underbrace{(0, 0, \ldots, 0, a, 0, 0, \ldots)}_{\bar{a}}$$

so

$$\Phi(x) = \sum r_a \Phi(\bar{a}) = \sum r_a \phi(a)$$

and since this expression for x is unique, Φ is unique and well-defined. ■

This is similar to the classic fact in linear algebra which states that linear maps over vector spaces are determined exactly by how the basis elements are mapped.

Example 3.110. *Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/4\mathbb{Z}$. Then M is not free. We can see this by trying to find a basis, or we can think about the homomorphism from*

$$\begin{aligned} \mathbb{Z}/4\mathbb{Z} &\to \mathbb{Z}/7\mathbb{Z} \\ 1 &\to \bar{0} \end{aligned}$$

Observe,

$$4 \cdot \bar{1} = \bar{0} \implies 4 \cdot \phi(\bar{1}) = \bar{0} \implies \phi(\bar{1}) = \bar{0}$$

Definition 3.111. *(Construction of $F(A)$). We can also define*

$$F(A) := \{\text{functions } f : A \to R : f(a) = 0 \text{ for all but finitely many } a \in A\}$$

equipped with the group operation and R-action

$$(f+g)(a) = f(a) + g(a)$$

$$(rf)(a) = rf(a)$$

We can prove this $F(A)$ satisfies the universal property stated previously.

Remark 3.112. *When R is commutative, $R(A) \cong F(A) \iff$ cardinality of A and B agree. However, in general, this relationship is not true. So rank need not be well-defined when R is noncommutative.*

Vazirani Prelim Trick: (Reduce it to linear algebra) If $\mathcal{M} \subset R$ is a maximal ideal, go to $R/\mathcal{M}$ which we know to be a field!

Example 3.113. *Let $R = \mathbb{Z}$. Pick your favorite prime p, say $p = 3$. Then*

$$\bigoplus_{a\in A} {}_{\mathbb{Z}}\mathbb{Z} = \bigoplus_{a\in A} \mathbb{Z}a = \bigoplus_{a\in A} Ra = F(A) \cong F(B) = \bigoplus_{b\in B} Rb = \bigoplus_{b\in B} \mathbb{Z}b = \bigoplus_{b\in B} {}_{\mathbb{Z}}\mathbb{Z}$$

Now, pass to $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$ and $F(A)/3F(A) = F(A)/3\mathbb{Z}\cdot F(A)$. We should check that $F(A)/3F(A) \cong \bigoplus_{a\in A} \mathbb{Z}/3\mathbb{Z}a$ is a $\mathbb{Z}/3\mathbb{Z}$-module.
Recall the stray fact that $I \subset R$ is an ideal implies $IM \subset M$ is a submodule, so M/IM is a quotient module is killed by I, so can be seen as an R/I-module. As a result, we get

$$\bigoplus_{a\in A} \mathbb{F}_3 a \cong \bigoplus_{b\in B} \mathbb{F}_3 b$$

and both of these are $\mathbb{F}_3$ vectors spaces. Therefore, by linear algebra, we see

$$|A| = |B|$$

Note 3.114. *This works for any commutative ring with maximal ideal $\mathcal{M}$.*

Lemma 3.115. *Given any ${}_RM$ and ring homomorphism $\phi : S \to M$, we can use ϕ to turn M into ${}_SM$ by defining*

$$s \cdot m = \phi(s) \cdot M$$

This is how we can go backwards $\pi : R \to R/I$ to turn R/I-modules into R-modules.

Note 3.116. *This also works for embeddings within rings with ϕ : subring $\to$ ring.*

Example 3.117. *If M is an $\mathbb{F}[x]$-module, it is also an $\mathbb{F}$-module. Since $\mathbb{F} \subset \mathbb{F}[x]$, we can define*

$$\begin{aligned} \phi : \mathbb{F} &\to \mathbb{F}[x] \\ c &\to c = c \cdot 1 + 0x + 0x^2 + \dots \end{aligned}$$

4 Tensors

4.1 Tensor Products on $\mathbb{F}$-Vector Spaces

Recall $\mathbb{F}^n \oplus \mathbb{F}^m \cong \mathbb{F}^{n+m}$. Also, given $\mathbb{F}$-linear maps,

$$g_1 : \mathbb{F}^{n_1} \to \mathbb{F}^{m_1} \qquad g_2 : \mathbb{F}^{n_2} \to \mathbb{F}^{m_2}$$

Then we can form

$$\begin{aligned} g_1 \oplus g_2 : \mathbb{F}^{n_1} \oplus \mathbb{F}^{n_2} &\to \mathbb{F}^{m_1} \oplus \mathbb{F}^{m_2} \\ (g_1 \oplus g_2)(v_1, v_2) &\to (g_1(v_1), g_2(v_2)) \end{aligned}$$

Placing this in the context of matrices, suppose g_1 and g_2 are linear maps with companion matrices A and B of dimensions $m_1 \times n_1$ and $m_2 \times n_2$ respectively. Then we see the matrix corresponding to $g_1 \oplus g_2$ is:

$$A \oplus B = \left[\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right]$$

So we can simply pick bases and "concatenate" or simply think of a new basis. If we consider $\mathbb{F}^{n_1} \times \mathbb{F}^{n_2}$, we have the basis

$$\mathcal{B} = \{(v_i, 0)\}_{i=1}^{n_1} \cup \{(0, w_j)\}_{j=1}^{n_2}$$

Question 4.1. *What is $\mathbb{F}^{n_1} \otimes \mathbb{F}^{n_2}$ as a tensor product?*

We want $\mathbb{F}^{n_1} \bigotimes \mathbb{F}^{n_2} \cong \mathbb{F}^{n_1 n_2}$ with basis

$$\mathcal{B} = \{v_1 \otimes w_j : 1 \leq i \leq n_1, 1 \leq j \leq n_2\}$$

Also, the elements of this new vector space are of the form

$$\sum_{i,j} a_{ij} v_i \otimes w_j$$

Further, we stipulate that $\otimes$ is "bilinear." Specifically, for any $v \in \mathbb{F}^{n_1} = V$ and $w \in \mathbb{F}^{n_2} = W$, then

$$v \otimes w = \left(\sum_{i=1}^{n_1} a_i v_i\right) \otimes \left(\sum_{j=1}^{n_2} b_j w_j\right) = \sum_{i,j} a_i b_j (v_i \otimes w_j)$$

with the operations defined as

$$\begin{aligned} (av + bv') \otimes w &= av \otimes w + bv' \otimes w \\ v \otimes (aw + bw') &= av \otimes w + bv \otimes w' \end{aligned}$$

Now to see this within the context of matrices, consider:

$$\begin{aligned} g_1 \otimes g_2 : \mathbb{F}^{n_1} \bigotimes \mathbb{F}^{n_2} &\to \mathbb{F}^{m_1} \bigotimes \mathbb{F}^{m_2} \\ (g_1 \otimes g_2)(v_i \otimes w_j) &\to g_1(v_i) \otimes g_2(w_j) \end{aligned}$$

Example 4.2. *Let* $A = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ *and* $B = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$*, then*

$$\begin{array}{c} \\ v_1 \otimes w_1 \\ v_1 \otimes w_2 \\ v_2 \otimes w_1 \\ v_2 \otimes w_2 \end{array} \begin{array}{c} \begin{array}{cc} v_1' \otimes w_1' & v_1' \otimes w_2' \end{array} \\ \left[\begin{array}{cc} 2 & 3 \\ 4 & 5 \\ 4 & 6 \\ 8 & 10 \end{array}\right] \end{array}$$

To see the underlying calculations:

$$A(v_1') = 1v_1 + 2v_2$$
$$B(w_1') = 2w_1 + 4w_2$$

$$\implies (A \otimes B)(v_1' \otimes w_1') = Av' \otimes Bw_1' = (1v_1 + 2v_2) \otimes (2w_1 + 4w_2) = 2v_1 \otimes w_1 + 4v_1 \otimes w_2 + 4v_2 \otimes w_1 + 8v_2 \otimes w_2$$

$$\implies (A \otimes B)(v_1' \otimes w_w') = Av' \otimes Bw_2' = (1v_1 + 2v_2) \otimes (3w_1 + 5w_2) = 3v_1 \otimes w_1 + 5v_1 \otimes w_2 + 6v_2 \otimes w_1 + 10v_2 \otimes w_2$$

Warning: The tensor product is usually much bigger than $V \oplus W$!
Now let's consider $V \bigotimes W$ via universal properties.

Definition 4.3. *Let U be another $\mathbb{F}$-vector space. Suppose we are given any bilinear map $\phi : V \times W \to U$. That is, a map ϕ that satisfies*

- $\phi(av + bv', w) = a\phi(v, w) + b\phi(v', w)$
- $\phi(v, aw + bw') = a\phi(v, w) + b\phi(v, w')$

Then $V \otimes W$ is the tensor product provided there exists an $\mathbb{F}$-linear map Φ such that

$$\begin{array}{ccc} V \times W & \xrightarrow{\ i\ } & V \otimes W \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \Phi} \\ & & U \end{array}$$

commutes with $i(v, w) = v \otimes w$ as a "simple tensor". That is,

$$\phi = \Phi \circ i$$

Lemma 4.4. *$V \otimes W$ with basis $v_i \otimes w_j$ is compatible with this universal property.*

Proof. To verify that our previous definition is compatible, suppose $\phi : V \times W \to U$ is a bilinear mapping. We can define Φ on the basis vectors

$$\begin{aligned} \Phi : \mathbb{F} - \text{span}\{v_i \otimes w_j\} &\to U \\ v_i \otimes w_j &\to \phi(v_i, w_j) \end{aligned}$$

which extends linearly since Φ is a $\mathbb{F}$-linear map. Now, observe

$$\phi(v, w) = \phi(\sum a_i v_i, \sum_j b_j w_j) = \sum_{i,j} a_i b_j \phi(v_i, w_j) = \sum_{i,j} a_i b_j \Phi(v_i \otimes w_j) = \Phi\left[\left(\sum_i a_i v_i\right) \otimes \left(\sum_j b_j w_j\right)\right] = \Phi(i(v, w))$$

$$\implies \phi = \Phi \circ i$$

Technically one should check this is unique. ∎

4.2 Tensor Products on Generalized Modules

For a free R-module, with R commutative, then we can define the tensor product in the same way! That is, get a free module with a basis constructed in the same way.

Definition 4.5. *Consider M_R, ${}_R N$ and ${}_{\mathbb{Z}} L$ modules. Then the mapping $\phi : M \times N \to L$ is <u>R-balanced</u> provided*

1. $\phi(m + m', n) = \phi(m, n) + \phi(m', n)$
2. $\phi(m, n + n') = \phi(m, n) + \phi(m, n')$

3. $\phi(mr, n) = \phi(m, rn)$

for all $m, m' \in M, n, n' \in N, r \in R$.

Definition 4.6. *Consider the modules* M_R, ${}_RN$ *over a commutative ring* R. *The tensor product over* R *of* M *and* N, *written* $M \otimes_R N$ *is the* $\mathbb{Z}$*-module satisfying the universal property:*

Given the R*-balanced inclusion mapping*

$$i : M \times N \to M \otimes_R N$$
$$(m, n) \to n \otimes n$$

then for any $\mathbb{Z}$*-module* L *as well as an any* R*-balanced* $\phi : M \times N \to L$, *there exists a unique* $\mathbb{Z}$*-module homomorphism* $\Phi : M \otimes_R N \to L$ *such that the diagram*

$$\begin{array}{ccc} M \times N & \xrightarrow{i} & M \otimes N \\ & \searrow^{\phi} & \downarrow \exists! \Phi \\ & & L \end{array}$$

commutes. Moreover,

$$\phi = \Phi \circ i$$

Theorem 4.7. *The tensor product over* R *of* M *and* N *is well-defined.*

Remark 4.8. $m \otimes 0 = 0 \otimes n = 0$ *is the zero of the* $\mathbb{Z}$*-module* $M \otimes_R N$.

Observation 4.9. *If you begin with* ${}_SM_R$, ${}_RN_T$, *then* $M \otimes_R N$ *is an* (S, T)*-bimodule structure. This is reminiscent of* $Hom_R({}_SM_R, {}_RN_T)$, *which is just a* $\mathbb{Z}$*-module without the* S, T *structure.*
Checking the actions, we see this is the same underlying set:

$$s \cdot \left(\sum m_i \otimes n_j \right) = \sum (s \cdot m_i) \otimes n_i$$
$$\left(\sum m_i \otimes n_j \right) \cdot t = \sum m_i \otimes (n_i \cdot t)$$

Observation 4.10. *So when* R *is commutative,* M_R *is automatically* ${}_RM_R$ *and so* $M \otimes_R N$ *gets an* R*-module structure. This can be seen by adjusting the universal property*

$$\begin{array}{ccc} M \times N & \xrightarrow{i} & M \otimes_R N \\ & \searrow^{\phi} & \downarrow \exists! \Phi \\ & & L \end{array}$$

To ${}_RL$ *and* Φ *are* R*-module maps, and change* ϕ *to be* R*-bilinear with*

$$\phi(rm, n) = r\phi(m, n) = \phi(m, rn)$$

Example 4.11. *Tensoring together* R_R *and* ${}_RM$, *we see* $R \otimes_R M \cong M$.

Example 4.12. *When* $R = \mathbb{Z}$,

$$\mathbb{Z}/m\mathbb{Z} \otimes_R \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/gcd(m, n)\mathbb{Z}$$

Example 4.13.

$$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \cong \{0\}$$

- *Method 1: Consists of taking sums of simple tensors. Consider* $\bar{1} \otimes \bar{1} = 3 \cdot \bar{1} \otimes \bar{1} = \bar{1} \otimes 3\bar{1} = \bar{1} \otimes \bar{0} = \bar{0} \otimes \bar{0} = 0$. *So for any* $\bar{a} \otimes \bar{b} = 0$.

- *Method 2: Using the universal property definition. Suppose we have any ϕ a $\mathbb{Z}$-balanced map.*

$$\begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \xrightarrow{\ i\ } & \{0\} \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \Phi} \\ & & L \end{array}$$

Observe,

$$\phi(\bar{a}, \bar{b}) = \phi(\bar{a} \cdot 3, \bar{b}) = \phi(\bar{a}, 3\bar{b}) = \phi(\bar{a}, \bar{0})$$
$$\phi(\bar{a}, \bar{b}) = \phi(\bar{a}, 4 \cdot \bar{b}) = \phi(4 \cdot \bar{a}, \bar{b}) = \phi(0, \bar{b})$$

and in L, we see:

$$\phi(\bar{a}, \bar{b}) + \phi(\bar{a}, \bar{0}) = \phi(\bar{a}, \bar{b} + \bar{0}) = \phi(\bar{a}, \bar{b})$$
$$\implies \phi(\bar{a}, \bar{0}) = 0$$

Therefore, ϕ is the 0-map. So we can simply choose Φ is also the 0-map.

Question 4.14. *Why can't we just use any module with the zero map?*

Fill-in

Example 4.15. $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}[x] \cong \mathbb{Z}/2\mathbb{Z}[x] = \mathbb{F}_2[x]$.

Example 4.16. $\mathbb{Q}[x]/\langle x-2\rangle \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/\langle x^3-1\rangle \cong \{0\}$.
Consider the simple tensor $\bar{f} \otimes \bar{g}$. Notice, we can decompose the unit of $\mathbb{Q}[x]$ by

$$1 = \frac{1}{7}(x^3 - 1) - \frac{1}{7}(x-2)(x^2 + 2x + 4)$$

So, by quick calculation, we see

$$\begin{aligned} \bar{f} \otimes \bar{g} &= \bar{f} \otimes 1\bar{g} = \bar{\otimes}(\frac{1}{7}(x^3-1) - \frac{1}{7}(x-2)(x^2+2x+4))\bar{g} \\ &= \bar{f} \otimes -\frac{1}{7}(x-2)(x^2+2x+4)\bar{g} \\ &= \bar{f}(x-2) \otimes -\frac{1}{7}(x^2+2x+4)\bar{g} \\ &= \bar{0} \otimes -\frac{1}{7}(x^2+2x+4)\bar{g} = 0 \end{aligned}$$

There is a whole class of examples for a ring S that is a right module of R. That is, ${}_S S_R$. When S is a ring, we can write:

$$S \otimes_R M$$

and is often called <u>an extension of scalars</u>. Further, if S_R is a free R-module, then $\otimes$ reduces significantly in complexity!

Example 4.17. $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[x] \cong \mathbb{C}[x]$

Example 4.18. $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{M}_3(\mathbb{Q}) \cong \mathbb{M}_3(\mathbb{C})$

Example 4.19. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[x] \cong \mathbb{Q}[x]$

Example 4.20. *If R, S are rings such that S_R is a right R-module and ${}_R M$ is a <u>free</u> R-module with basis $\{m_j\}$, then $S \otimes M$ is a free S-module with basis $\{1 \otimes m_j\}$*

Example 4.21. $\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}[x] \cong \mathbb{Z}/3\mathbb{Z}[x]$ *with basis* $\{1, x, x^2, x^3, \ldots\}$

Example 4.22. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \cong \{0\}$

Example 4.23. *If R is a commutative ring, then $R/I \otimes_R M \cong M/IM$.*

Example 4.24. *$I \otimes_R M \cong IM$. Should remind yourself of the ideal*

$$IJ = \left\{ \sum a_i b_i : a_i \in I, b_i \in J \right\}$$

Theorem 4.25 (Existence/ Construction)**.** *Let F be the free $\mathbb{Z}$-module on $A = M \times N$. Let S be the $\mathbb{Z}$-submodule of F generated by all elements of the form:*

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n)$$

$$(m, n_1 + n_2) - (m, n_1) - (m, n_2)$$

$$(mr, n) - (m, rn)$$

for all $m, m_1, m_2 \in M, n, n_1, n_2 \in N, r \in R$. Then F/S satisfies the universal property for the tensor product of M and N, with

$$\begin{array}{ccccc} M \times N & \xrightarrow{i} & F & \xrightarrow{\pi} & F/S \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \tilde{\phi}} & \swarrow_{\exists! \Phi} & \\ & & L & & \end{array}$$

for any R-balanced ϕ mapping to a $\mathbb{Z}$-module L. Moreover, $\tilde{\phi}$ factors through F/S to result in the commutative diagram:

$$\begin{array}{ccc} M \times N & \xrightarrow{i} & F/S \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \Phi} \\ & & L \end{array}$$

with $\phi = \Phi \circ i$. Uniqueness comes from leveraging the freeness of F.

Theorem 4.26. *Suppose $R \subset S$ a subring, L an S-module, N an R-module, and*

$$i : N \to S \otimes_R N$$
$$n \to 1 \otimes n$$

Then for any given $\phi \in Hom_R(N, Res^S_R L)$, there exists a unique $\Phi \in Hom_S(S \otimes_R N, L)$ such that the diagram

$$\begin{array}{ccc} N & \xrightarrow{i} & S \otimes_R N \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \Phi} \\ & & L \end{array}$$

commutes. Moreover, $\phi = \Phi \circ i$.

Remark 4.27. *We can recast this theorem into the context of $\mathbb{Z}$-modules.*

$$Hom_R(N, Res^S_R L) \cong Hom_S(S \otimes_R N, L)$$

Remark 4.28. *If S is a k-algebra, this is an isomorphism over k-algebras.*

Remark 4.29. *Often call a functor a mapping $N \to S \otimes_R N = Ind^S_R N$. This says induction is a left 1-sided adjoint to restriction.*

Now recall for vector spaces ${}_{\mathbb{F}}V/$ matrices, we could tensor the maps. There is an analogous process for ${}_R M$.

Theorem 4.30. *Let consider the modules $M_R, M'_R, {}_R N$, and ${}_R N'$. Let $\phi \in Hom_R(M_R, M'_R)$ and $\psi \in Hom_R({}_R N, {}_R N')$.*

1. *$\phi \otimes \psi \in Hom_{\mathbb{Z}}(M \otimes_R N, M' \otimes_R N)$ is defined via*

$$(\phi \otimes \psi)(m \otimes n) = \phi(m) \otimes \psi(n)$$

2. *If there is an appropriate bimodule structure, this also works for $\phi \in Hom_S(M, M')$, so $\phi \circ \psi$ is a homomorphism of left S-modules. If R is commutative, then $\phi \otimes \psi$ is an R-module homomorphism.*

3. *(Composition) If $\lambda : M'_R \to M''_R$ and $\mu : {}_RN' \to {}_RN''$, then*

$$(\lambda \otimes \mu) \circ (\phi \otimes \psi) = (\lambda \circ \phi) \otimes (\mu \circ \psi)$$

Proof. 1. Define $M \times N \xrightarrow{\phi} M' \otimes_R N'$ by

$$(m, n) \xrightarrow{\phi} \phi(m) \otimes \psi(n)$$

and show that ϕ is R-balanced in order to yield

$$\Phi : M \otimes_R N \to M' \otimes_R N'$$

■

Theorem 4.31 (Associativity of $\otimes$)**.** *Given appropriate bimodules $M_R, {}_RN_T, {}_TL$, then*

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

as $\mathbb{Z}$-modules. On simplie tensors, this appears as

$$(m \otimes n) \otimes \ell \to m \otimes (n \otimes \ell)$$

Proof. Exercise ■

In case $T = R$ is commutative, then this motivates replacing the bilinear requirement with an R-multilinear mapping.

Definition 4.32. *Let R be commutative, and let M_i, L be R-modules. Then $\phi : M_1 \times M_2 \times \ldots \times M_n$ is <u>R-multilinear</u> if it is additive in each coordinate an*

$$\phi(m_1, m_2, \ldots, rm_i, \ldots, m_n) = r\phi(m_1, m_2, \ldots, m_i, \ldots, m_n)$$

Definition 4.33. *Define $M_1 \otimes M_2 \otimes \ldots \otimes M_n$ over R with*

$$i(m_1, m_2, \ldots, m_n) = m_1 \otimes m_2 \otimes \ldots \otimes m_n$$

to be universal with respect to a given multilinear map ϕ, there exists a unique R-module homomorphism Φ such that the diagram

$$\begin{array}{ccc} M_1 \times M_2 \times \ldots \times M_n & \xrightarrow{i} & M_1 \otimes M_2 \otimes \ldots \otimes M_n \\ & \searrow^{\phi} & \downarrow \exists! \Phi \\ & & L \end{array}$$

commutes.

Theorem 4.34. $(M_1 \oplus M_2) \otimes_R N \cong M_1 \otimes_R N \oplus M_2 \otimes_R N$

$$M \otimes_R (N_1 \oplus N_2) \cong M \otimes_R N_1 \oplus M \otimes_R N_2$$

Likewise, we can extend this to non-finite direct products:

$$M \otimes_R (\bigoplus_{i \in I} N_i) \cong \bigoplus_{i \in I} M \otimes_R N_i$$

Remark 4.35. *This fails for $\prod$. That is,*

$$M \otimes_R (\prod_{i\in I} N_i) \ncong \prod_{i\in I} M \otimes_R N_i$$

when $|I| = \infty$.

Corollary 4.35.1. *Let R be commutative. If M_i is free of rank r_i, equipped with basis $\{v_j^{(i)} : j \in J_i\}$, then $M_1 \otimes_R M_2$ is a free R-module of rank $r_1 r_2$ with basis*

$$\{v_j^{(1)} \otimes v_k^{(2)} : j \in J_1, k \in J_2\}$$

Proposition 4.36. *Let R be commutative with modules ${}_RM, {}_RN$.*

$$M \otimes_R N \cong N \otimes_R M$$

which is well-defined via the R-module homomorphism

$$m \otimes n \to n \otimes m$$

Proposition 4.37. *Suppose A, B are R-algebras, with R commutative. Then $A \otimes_R B$ is an R-algebra with multiplication operation*

$$(A \otimes b)(a' \otimes b') = aa' \otimes bb'$$

Example 4.38. *$R = \mathbb{Q}$ and $A = \mathbb{C}, B = \mathbb{M}_2(\mathbb{Q})$. Then*

$$\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{M}_2(\mathbb{Q}) \cong \mathbb{M}_2(\mathbb{C})$$

is still a $\mathbb{Q}$-algebra. Notice,

$$\begin{pmatrix} 1 & i \\ 2-i & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} + i \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Remark 4.39. *Let $J \subset R$ be an ideal and M and R-module. Notice $J \otimes_R M \ncong JM$*

Example 4.40. *$2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \neq \{0\}$ while $(2\mathbb{Z})(\mathbb{Z}/2\mathbb{Z}) = JM = \{0\}$. By our intuition, we remember ${}_{\mathbb{Z}}2\mathbb{Z}$ is a free module of rank 1, while $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$ module. So we would expect a rank 1 $\mathbb{Z}/2\mathbb{Z}$ module.*
We can show this by the universal property:

$$\begin{array}{ccc} 2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\ i\ } & \mathbb{Z}/2\mathbb{Z} \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \Phi} \\ & & N \end{array}$$

with N a $\mathbb{Z}$-module and ϕ is $\mathbb{Z}$-balanced. Checking our $\mathbb{Z}$-balanced mapping,

$$\phi(z, \bar{1}) = \phi(2, \bar{1}) + \phi(2, \bar{1}) = \phi(2, \bar{0}) = 0$$

Moreover, by the biadditivity of ϕ, we know ϕ is determined by $\phi(2, \bar{1})$ which gives us:

$$\phi(2n, \bar{0}) = 0$$

$$\phi(4n, \bar{0}) = 0$$

$$\phi(2(2m+1), \bar{1}) = \phi(2, \bar{1})$$

So the image of ϕ is $\langle \phi(2, \bar{1}) \rangle$. Therefore, we can define:

$$\begin{aligned} \Phi : \mathbb{Z}/2\mathbb{Z} &\to N \\ \Phi(\bar{1}) &= \phi(2, \bar{1}) \\ \Phi(0) &= 0 \end{aligned}$$

Proposition 4.41. *Suppose A, B are R-algebras. Then $A \otimes_R B$ is an R-algebra with multiplication defined*

$$(a \otimes b)(a' \otimes b')aa' \otimes bb'$$

Example 4.42. *Let $R = \mathbb{Q}, A = \mathbb{C}, B = \mathbb{M}_2(\mathbb{Q})$. Then*

$$\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{M}_2(\mathbb{Q}) \cong \mathbb{M}_2(\mathbb{C})$$

is still a $\mathbb{Q}$-algebra.

Note 4.43. *We can always decompose matrices in $\mathbb{M}_2(\mathbb{C}) = \mathbb{M}_2(\mathbb{Q}) + i\mathbb{M}_2(\mathbb{Q})$*

$$\begin{pmatrix} 1 & i \\ 2-i & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} + i \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and can be written

$$1 \otimes \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} + i \otimes \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Notice, this can ease matrix multiplication with

$$\left(1 \otimes \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} + i \otimes \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right)\left(1 \otimes \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} + i \otimes \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = 1{\cdot}1 \otimes \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} + i1 \otimes \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \dots$$

Example 4.44. *When R is commutative, $M \otimes_R N \cong N \otimes_R M$. Suppose ϕ an R-balanced map from $M \times N \to A$ with A a $\mathbb{Z}$-module. We want to identify Φ such that the diagram commutes:*

$$\begin{array}{ccc} M \times N & \xrightarrow{\ i\ } & N \otimes_R M \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \Phi} \\ & & A \end{array}$$

Specifically, we would need

$$\Phi(n \otimes m) = \phi(m, n)$$

to extend linearly. This requires us to check that biadditivity holds for this mapping. Observe,

$$\Phi((n_1 + n_2) \otimes m) = \phi(m, n_1) + \phi(m, n_2)$$

$$\Phi(nr \otimes m) = \Phi(n \otimes rm)$$

which this latter relation requires R to be commutative. Might think we need to check well-definedness in a broad sense. That is,

$$n \otimes m = \sum_i n_i \otimes m_i$$

Then by the linear extension of Φ, we see that

$$\begin{aligned} \Phi(n \otimes m) &= \Phi\left(\sum_i n_i \otimes m_i\right) \\ &= \sum_i \Phi(n_i \otimes m_i) \\ &= \sum_i \phi(m_i, n_i) \end{aligned}$$

But this calculation is unnecessary, since we have shown the relations hold on the simple tensors. We could have also gone through the calculation

$$\begin{array}{ccc} M \times N & \xrightarrow{\ i\ } & M \otimes_R N \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \Phi} \\ & & N \otimes_R M \end{array}$$

and shown that in fact Φ is an isomorphism. Both ways work!

Example 4.45. $\mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{R}[x] \cong \mathbb{R}[x, y]$

- *Intuitive Approach:* *We know that* ${}_{\mathbb{R}}\mathbb{R}[x] \cong {}_{\mathbb{R}}\mathbb{R}[y]$. *Therefore, we see that*

$$\begin{aligned} f(x) \otimes g(y) &= (a_0 + a_1 x + \ldots) \otimes (b_0 + b_1 y + \ldots) \\ &= a_0 b_0 1 \otimes 1 + b_0 a_1 x \otimes 1 + a_0 b_1 1 \otimes y + a_1 b_1 x \otimes y + \ldots \end{aligned}$$

Therefore, we see that each tensor $f(x) \otimes g(y)$ *can be mapped to something of the form* $\sum_{i,j} a_i b_j x_i y_j \in \mathbb{R}[x, y]$. *Specifically, we see through the calculation of the monomials:*

$$(x^i \otimes y^j)(x^m \otimes y^n) = x^i x^m \otimes y^j y^n$$

We can see the connection to:

$$\begin{gathered} \mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{R}[x] \cong \mathbb{R}[y, z] \\ x \otimes 1 \leftrightarrow y \\ 1 \otimes x \leftrightarrow z \end{gathered}$$

Notice, $yz = zy$ *since* $x \otimes x = (x \otimes 1)(1 \otimes x) = (1 \otimes x)(x \otimes 1)$

- *Universal Property:* *Consider the diagram:*

$$\begin{array}{ccc} \mathbb{R}[x] \times \mathbb{R}[x] & \xrightarrow{\ i\ } & \mathbb{R}[y, z] \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \Phi} \\ & & {}_{\mathbb{R}}N \end{array}$$

where ϕ *is* $\mathbb{R}$*-bilinear. Notice,* ϕ *is determined by* $\phi(x^k, x^j)$ *since*

$$a\phi(x^k, x^j) = \phi(ax^k, x^j) = \phi(x^k, ax^j)$$

Therefore, since $i(x^k, x^k) = y^k z^j$, *we can set*

$$\Phi(y^k z^j) = \phi(x^k, x^j)$$

and extend linearly since $\{y^k z^j\}$ *us an* $\mathbb{R}$*-basis. Moreover,* Φ *is forced to be unique.*

Example 4.46. $\mathbb{Q}(\omega) \otimes_{\mathbb{Q}} \mathbb{Q}(\omega) \cong \mathbb{Q}(\omega) \times \mathbb{Q}(\omega)$ *as* $\mathbb{Q}$*-algebras and as* $\mathbb{Q}(\omega)$*-algebras.*
Since these are vector spaces, we can leverage our pre-existing knowledge on vector spaces. Recall from Galois theory that $\mathbb{Q}(\omega) \cong \mathbb{Q}[x]/\langle x^2 + x + 1 \rangle$. *Then*

$$\mathbb{Q}(\omega) \otimes_{\mathbb{Q}} \mathbb{Q}(\omega) \cong \mathbb{Q}(\omega) \otimes_{\mathbb{Q}} \mathbb{Q}[x]/\langle x^2+x+1 \rangle \cong \mathbb{Q}(\omega)[x]/\langle x^2+x+1 \rangle \cong \mathbb{Q}(\omega)[x]/\langle x-\omega \rangle \times \mathbb{Q}(\omega)[x]/\langle x-\bar{\omega} \rangle \cong \mathbb{Q}(\omega) \times \mathbb{Q}(\omega)$$

Example 4.47. $\mathbb{C}[\mathbb{S}_3] \otimes_{\mathbb{C}[A_3]} \mathbb{C}$

Example 4.48. $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = \{0\}$ *since for any simple tensor*

$$\frac{a}{b} \otimes \frac{c}{d} = \frac{ad}{bd} \otimes \frac{c}{d} = \frac{a}{bd} \otimes c = \frac{a}{bd} \otimes 0 = 0$$

To see this using the universal property, consider any $\mathbb{Z}$*-balanced mapping* $\phi : \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z} \to {}_{\mathbb{R}}N$. *Clearly,*

$$\phi(\frac{a}{b}, \frac{c}{d}) = \phi(\frac{a}{bd}, 0) = 0$$

So the only possible diagram to satisfy the universal property is:

$$\begin{array}{ccc} \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z} & \xrightarrow{\ i\ } & 0 \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \Phi} \\ & & N \end{array}$$

This is similar to the example $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$.

Example 4.49. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$ *since* $i(x,y) = xy$ *is a* $\mathbb{Z}$*-balanced mapping with* $\Phi(r) = \phi(r,1)$*. Then we see that*

$$\Phi \circ i(x,y) = \Phi(xy) = \phi(xy,1) = \phi(x,y)$$

and the diagram

$$\begin{array}{ccc} \mathbb{Q} \times \mathbb{Q} & \xrightarrow{\ i\ } & \mathbb{Q} \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \Phi} \\ & & N \end{array}$$

commutes!

4.3 Tensor Algebras

Definition 4.50. *Suppose* R *is commutative. Given* ${}_RM$*, a* tensor algebra*, denoted* $\mathcal{T}(M)$*, which is defined recursively by:*

- $\mathcal{T}^0(M) = R$
- $\mathcal{T}^1(M) = M$
- $\mathcal{T}^k(M) = \underbrace{M \otimes_R M \otimes_R M \otimes_R \ldots \otimes_R M}_{k \text{ times}}$

Then

$$\mathcal{T}(M) := \bigoplus_{k \geq 0} \mathcal{T}^k(M)$$

Proposition 4.51. $\mathcal{T}(M)$ *is an* R*-algebra with the multiplication operation defined to be "concatenation", which is the mapping*

$$(m_1 \otimes \ldots \otimes m_i)(m_1' \otimes \ldots \otimes m_j') = m_1 \otimes \ldots \otimes m_i \otimes m_1' \otimes \ldots \otimes m_j'$$

We can also define Tensor Algebras using the universal property.

Definition 4.52. *(Universal Property of the Tensor Algebra) If* A *is any* R*-algebra and* $\phi : M \to A$ *is an* R*-module homomorphism, then there is a unique* R*-algebra homomorphism* $\Phi : \mathcal{T}(M) \to A$ *such that* $\Phi|_M = \phi$*. Notice,* $M = \mathcal{T}^1(M) \subset \mathcal{T}(M)$*.*

Example 4.53. $R = \mathbb{R}$ *with* $M = \mathbb{F}^1$*. Then* $\mathcal{T}(M) \cong \mathbb{F}[x]$*. To see this, observe,*

$$\mathcal{T}^i(M) = \mathbb{F} \otimes_{\mathbb{F}} \mathbb{F} \otimes_{\mathbb{F}} \ldots \otimes_{\mathbb{F}} \mathbb{F} \cong \mathbb{F}$$

Therefore, we see that

$$\mathcal{T}^0(M) = \mathbb{F} \leftrightarrow 1$$
$$\mathcal{T}^1(M) = \mathbb{F} \leftrightarrow x$$
$$\mathcal{T}^2(M) = \mathbb{F} \leftrightarrow x^2$$
$$\ldots$$
$$\mathcal{T}^i(M) = \mathbb{F} \leftrightarrow x^i$$

Therefore, we can easily imagine an isomorphism between $\mathcal{T}(M) \cong \mathbb{F}[x]$*.*

Example 4.54. $R = \mathbb{F}, M = \mathbb{F}^2$*. We see:*

$$\mathcal{T}^1(M) \text{ has basis } v, w$$
$$\mathcal{T}^2(M) \text{ has basis } v \otimes w, w \otimes v, v \otimes v, w \otimes w$$

$$\mathcal{T}^i(M) = \underbrace{\mathbb{F}^2 \otimes_{\mathbb{F}} \mathbb{F}^2 \otimes_{\mathbb{F}} \ldots \otimes_{\mathbb{F}} \mathbb{F}^2}_{i \text{ times}} \text{ has dimension } 2^i$$

If the basis of $\mathbb{F}^2$ *is* $\{x_1, x_2\}$*, then* $\mathbb{F}^2 \otimes \mathbb{F}^2$ *has basis,*

$$x_1 \otimes x_1, x_1 \otimes x_2, x_2 \otimes x_1, x_2 \otimes x_2$$

So $(\mathbb{F}^2)^{\otimes i}$ *has basis*

$$x_{k_1} \otimes x_{k_2} \otimes \ldots \otimes x_{k_i}$$

where $k_j \in \{1, 2\}$*. These basis elements are the worlds in* x, y *of length* i*.*

This is an example of noncommutative polynomial algebra over $\mathbb{F}$*. In this case, we write*

$$\mathcal{T}(M) = \mathbb{F}\langle x, y\rangle$$

Further, this extends similarly for $M = \mathbb{F}^n$ *with* $dim(\mathcal{T}^k(\mathbb{F}^n)) = n^k$ *and* $\mathcal{T}(M) = \mathbb{F}\langle x_1, \ldots, x_n\rangle$*.*

Example 4.55. *Let* $R = \mathbb{Z}, M = \mathbb{Z}/3\mathbb{Z}$*. Then*

$$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$$

So

$$\mathcal{T}(\mathbb{Z}/3\mathbb{Z}) = \mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \ldots$$

We can further realize this as a ring by $\mathbb{Z}[x]/\langle 3x\rangle$*.*

Example 4.56. *Let* $R = \mathbb{Z}, M = \mathbb{Z}/3\mathbb{Z}$*. Let* $A = \mathbb{M}_2(\mathbb{Z}/3\mathbb{Z})$ *is a* $\mathbb{Z}$*-algebra. Moreover, define*

$$f_1 : \mathbb{Z}/3\mathbb{Z} \to A$$
$$a \to \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

$$f_2 : \mathbb{Z}/3\mathbb{Z} \to A$$
$$b \to \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix}$$

as $\mathbb{Z}$*-module maps. The universal property tells us that these can be extended via some functions* $F_1, F_2 : \mathbb{T}(\mathbb{Z}/3)\mathbb{Z} \to A$*. Observe:*

Degree:	F_1	F_2
0	$n \to \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}$	$n \to \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}$
1	$a \to \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$	$b \to \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix}$
2	$a_1 \otimes a_2 \to \begin{pmatrix} a_1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1a_2 & 0 \\ 0 & 0 \end{pmatrix}$	$b_1 \otimes b_2 \to \begin{pmatrix} 0 & 0 \\ b_1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ b_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

This yields the ring homomorphisms:

$$n + \overline{f(x)} \xrightarrow{F_1} \begin{pmatrix} \bar{n} + \overline{f(1)} & 0 \\ 0 & \bar{n} \end{pmatrix}$$

$$n + b_1x + b_2x^2 + \ldots \xrightarrow{F_2} \begin{pmatrix} \bar{n} & 0 \\ b_1 & \bar{n} \end{pmatrix}$$

Definition 4.57. *Let S be a ring. S is a graded ring if*

$$S = S_0 \oplus S_1 \oplus S_1 \oplus S_2 \oplus \dots$$

such that S_i is a $\mathbb{Z}$-submodule and $S_iS_j \subset S_{i+j}$ for all $i, j \in \mathbb{N}$. S_k is called the homogenous component of degree k and any nonzero element $a \in S_k$ is (homogenous of) degree k.

Definition 4.58. *An ideal $I \subset S$ of a graded ring is a graded ideal if $I = \bigoplus_{k\geq 0}(I \cup S_k)$.*

Definition 4.59. *Let S, T be graded rings. $\phi : S \to T$ is an homomorphism of graded rings if ϕ is a ring homomorphism such that $\phi(S_k) \subset T_k$.*

Note 4.60. *Need not grade by $\mathbb{N}$. We can also grade via any abelian group A such that*

$$S_aS_b \subset S_{a+b}$$

for any $a, b \in A$. You can even go so far as to define using a semigroup, but this is beyond the scope of this course.

Example 4.61. *Let $A = \mathbb{N} \times \mathbb{N}$ for $\mathbb{R}[x, y]$ with $deg(x) = (1, 0)$ and $deg(y) = (0, 1)$.*

Example 4.62. *$\mathcal{T}(M)$ is a graded ring.*

Example 4.63. *$S = \mathbb{F}[x]$ is a graded ring with degree $x^k = k$ and degree $ax^k = k$ for any $a \in \mathbb{F}^{\times\cdot}$ Further, $I = \langle x^3 \rangle$ is a graded ideal. And we see that*

$$I \cap S^0 = \{0\}$$
$$I \cap S^1 = \{0\}$$
$$I \cap S^2 = \{0\}$$
$$I \cap S^3 = \mathbb{F} \cdot x^3$$
$$I \cap S^4 = \mathbb{F} \cdot x^4$$
$$\dots$$

Taking the direct sum of these allows us to recover I.

Example 4.64. *$I = \langle x - 1 \rangle$ is NOT a graded ideal. Observe,*

$$gcd(x^k, x - 1) = 1$$

for all choices of k. Therefore, $I \cap S^k = \{0\}$ for all k. Therefore, we see that

$$I \neq \bigoplus_{k\geq 0}(I \cap S^k)$$

On the other hand, any ideal generated by homogenous elements will be graded:

$$I = \langle x^3 \rangle = \langle x^3 + x^4, x^3 - x^4 \rangle$$

Example 4.65. *Let $T = \mathbb{F}$ is a graded ring with $T_0 = \mathbb{F}, T_k = 0$ for $k < 0$. Define the mapping:*

$$\phi : \mathbb{F}[x] \to \mathbb{F}$$
$$x \to 0$$
$$a \to a, a \in \mathbb{F}$$

Then we see that this is equivalent to evaluation at $x = 0$. So $\phi(S_k) = 0 = T_k$. But on the other hand, for the mapping

$$\psi : \mathbb{F}[x] \to \mathbb{F}$$
$$f(x) \to f(2)$$

is not with $\psi(x) = 2, x \in S_1, 2 \in T_0$. But $2 \notin T_1$. So we see that $Ker(\phi) = \langle x \rangle$ is a graded ideal but $Ker(\psi) = \langle x-2 \rangle$ is not a graded ideal.

Proposition 4.66. *Let $S = \bigoplus_{k\geq 0} S_k$ be a graded ring with $I = \bigoplus_{k\geq 0} I_k = I \cap S_k$ be a graded ideal. Then S/I is a graded ring with*

$$(S/I)_k = S_k/I_k$$

Proof. Notice that

$$S/I = \bigoplus_{k\geq 0} S_k/I_k$$

which follows from the results of studying Abelian groups. Now we simply need to check that multiplication is upheld:

$$(a + I_k)(b + I_j) = \underbrace{ab}_{S_{k+j}} + \underbrace{I_k b + aI_j + I_k I_j}_{\subset I_{k+j}} = ab + I_{j+k}$$

To see that $I_k b + aI_j + I_k I_j \subset I_{k+j}$, we recall that $I_k b \subset I$ since I is an ideal. Also $I_k b \subset S_{k+j}$ since it is graded. Therefore, $I \cap S_{k+j} = I_{k+j}$. The same argument can be made for the other terms.
Therefore, $(a + I_k)(b + I_j) \in S_{k+j}/I_{k+j}$. ■

Theorem 4.67. *If ϕ is a homomorphism of graded rings, then $Ker\phi$ is a graded ideal.*

Proof. Let $\phi : S \to T$ be a graded ring homomorphism. If $\phi(a) = 0$, we can write

$$a = \sum_k a_k$$

with $a_k \in S_k$ so

$$0 = \sum_k \underbrace{\phi(a_k)}_{T_k} \in \bigoplus_k T_k$$

So the only way to write 0 is as $0 = 0 + 0 + \ldots + 0$. So each $\phi(a_k) = 0$. Therefore, $a_k \in Ker\phi \cap S_k$. Therefore,

$$Ker\phi = \bigoplus_k Ker\phi \cap S_k$$

■

Remark 4.68. *We can extend the first, second, third and correspondence theorems of rings to graded rings in particular.*

Definition 4.69. *Let R be a commutative ring. Given ${}_R M$, the $\underline{\mathcal{C}(M)}$ is the set of 2-sided ideals in $\mathcal{T}(M)$ generated by $m_1 \otimes m_2 - m_2 \otimes m_1$.*

4.4 Symmetric Algebras

Proposition 4.70. *$\mathcal{C}(M)$ is graded.*

Proof.

$$\mathcal{C}^0 = 0 = \mathcal{C}^1(M)$$

$$\mathcal{C}^2 = \text{ sums of } m_1 \otimes m_2 - m_2 \otimes m_1$$

$$\mathcal{C}^3 = \text{ sums of } m \otimes m_1 \otimes m_2 - m \otimes m_2 \otimes m_1 \text{ and } m_1 \otimes m_2 \otimes m - m_2 \otimes m_1 \otimes m$$

■

Remark 4.71. *In general, if and ideal is generated by homogenous elements, it will be graded.*

Remark 4.72. *The symmetric group $\mathcal{S}_n$ is generated by the transpositions $s_1 = (1, 2), s_2 = (2, 3), \ldots, s_{n-1} = (n - 1, n)$.*

Therefore, we can define the general grade of $\mathcal{C}^n(M)$ to be generated by the elements of the form:

$$m_1 \otimes m_2 \dots m_n - m_{\sigma(1)} \otimes m_{\sigma(2)} \otimes \dots \otimes m_{\sigma(n)}$$

for all $\sigma \in \mathcal{S}_n$.

Definition 4.73. *The symmetric algebra $\mathcal{S}(M)$ is defined as*

$$\mathcal{S}(M) = \mathcal{T}(M)/\mathcal{C}(M)$$

It is a graded ring with $\mathcal{S}^k(M) = \mathcal{T}^k(M)/\mathcal{C}^k(M)$.

$$\begin{array}{ll} k=0 & \mathcal{S}^0(M) = \mathcal{T}^0/\mathcal{C}^0(M) = R \\ k=1 & \mathcal{S}^1(M) = \mathcal{T}^1/\mathcal{C}^1(M) = M/0 = M \\ k=2 & \mathcal{S}^2(M) = \mathcal{T}^2/\mathcal{C}^2(M) = M \otimes_R M/\langle m_1 \otimes m_2 - m_2 \otimes m_1 \rangle \end{array}$$

Notice $\mathcal{S}(M)$ is a commutative ring. We often write $m_1 m_2$ for $\overline{m_1 \otimes m_2}$ and $m_2 m_1$ for $\overline{m_2 \otimes m_1}$

Example 4.74. *Let $R = \mathbb{F}$ and $M = \mathbb{F}^1$. Recall $\mathcal{T}(M) \cong \mathbb{F}[x]$. But $\mathcal{C}(M) = \{0\}$. To see this, observe,*

$$m_1 \otimes m_2 - m_2 \otimes m_1 = a_1 x \otimes a_2 x - a_2 x \otimes a_1 x = (a_1 a_2 - a_2 a_1) x \otimes x = 0 x \times x = 0$$

So $\mathcal{S}(M) = \mathcal{S}(\mathbb{F}) = \mathcal{T}(\mathbb{F}) \cong \mathbb{F}[x]$.

Example 4.75. *Let $M = \mathbb{F}^2$ with basis x, y. Then $\mathcal{T}(M) = \mathbb{F}\langle x, y \rangle$. Then*

$$(a_1 x + b_1 y) \otimes (a_2 x + b_2 y) - (a_2 x + b_2 y) \otimes (a_1 x + b_1 y) = a_2 b_1 y \otimes x - a_1 b_2 y \otimes x + a_1 b_2 x \otimes y - a_2 b_1 x \otimes y = (a_1 b_2 - a_2 b_1)(x$$

So $\mathcal{C}^2(M) = span(x \otimes y - y \otimes x)$. Therefore, $\mathcal{S}^2(M)$ is spanned by xx, xy, yy.
$\mathcal{C}^3(M) = span(x \otimes x \otimes y - x \otimes y \otimes x, x \otimes y \otimes x - y \otimes x \otimes x)$.
Therefore, $\mathcal{S}(M) \cong \mathbb{F}[x, y]$.

Definition 4.76. *(Universal Property for Symmetric Multilinear Maps) If $\phi : M \times M \times \dots \times M \to N$ is a symmetric k-multilinear map over R, then there is a unique R-module $\Phi : \mathcal{S}^k(M) \to N$ such that $\phi = \Phi \circ i$, where*

$$\begin{aligned} i : M \times \dots \times M &\to \mathcal{S}^k(M) \\ m_1, \dots, m_k &\to m_1 \otimes \dots \otimes m_k \mod \mathcal{C}(M) \end{aligned}$$

Theorem 4.77. *(Universal Property for maps to commutative R-algebras) If A is any commutative R-algebra, and $\phi : M \to A$ is an R-module homomorphism, then there is an unique R-algebra homomorphism $\Phi : \mathcal{S}(M) \to A$ such that $\Phi|_M = \phi$.*

Proof. Given an R-module homomorphism $\phi : M \to A$ where A is a commutative R-algebra. We know we get a unique $\tilde{\Phi} : \mathcal{T}(M) \to A$ which is an R-module homomorphism. Since A is commutative

$$\mathcal{C}(M) \subset Ker(\tilde{\Phi})$$

So we can factor through $\mathcal{C}(M)$, which induces $\Phi : \mathcal{S}(M) \to A$. This also inherits uniqueness via $\mathcal{T}(M) \to \mathcal{S}(M) \to A$. ■

Corollary 4.77.1. *Let $\mathbb{F}$ be a field, $dim_{\mathbb{F}}(V) = n$ with basis $\{v_1, \dots, v_n\}$. Then we have the very nice way to realize $\mathcal{S}(V)$, specifically,*

$$\mathcal{S}(V) \cong \mathbb{F}[x_1, \dots, x_n]$$

by identifying $v_i \leftrightarrow x_i$. Also,

$$\mathcal{S}^k(V) = \text{ span of homogenous degree } k \text{ polynomials}$$

with $dim_{\mathbb{F}}(\mathcal{S}^k(V)) = \binom{k+n-1}{n-1}$.

Proof.
- In degree 0, $\implies$ 1 basis element of $\{1\}$
- In degree 1, we have exactly $\{x_1, x_2, \ldots, x_n\}$ are the basis elements. Moreover,
$$\binom{1+n-1}{n-1} = \binom{n}{n-1} = n$$
- In degree 2, we have exactly $\{x_i x_j : i \leq j\}$ basis elements, which is the formula for $(n+1)n/2 = \binom{2+n-1}{n-1}$.
- We can leverage the stars and bars argument to prove this in higher dimensions.

■

4.5 Exterior Algebras

Definition 4.78. *Let R be a commutative ring, ${}_RM$. Then the graded ideal $\mathcal{A}(M) \subset \mathcal{T}(M)$ is the ideal generated by*
$$\mathcal{A}(M) = \langle m \otimes m : m \in M \rangle$$

Definition 4.79. *The exterior algebra $\bigwedge(M) = \mathcal{T}(M)/\mathcal{A}(M)$.*

Note 4.80. *This algebra comes with a $\wedge$ notation, which simply means*
$$m_1 \wedge m_2 \wedge \ldots \wedge m_k = m_1 \otimes m_2 \otimes \ldots \otimes m_k + \mathcal{A}(M)$$

Definition 4.81. $\bigwedge^k(M) :=$ *the kth exterior power of M.*

Remark 4.82. *$\mathcal{A}(M)$ is a graded ring since each $m \otimes m$ is homogenous of degree 2. Moreover, we see that*
$$\mathcal{A}^0(M) = 0 \qquad \bigwedge^0(M) = R = \mathcal{T}^0(M)$$
$$\mathcal{A}^1(M) = 0 \qquad \bigwedge^1(M) = M = \mathcal{T}^1(M)$$
$$\mathcal{A}^2(M) = \text{ sums of all } m \otimes m$$

Observation 4.83. *For any $(m_1 + m_2) \otimes (m_1 + m_2) \in \mathcal{A}(M)$, we see that since $\mathcal{A}(M)$ is a closed module*
$$\underbrace{m_1 \otimes m_1}_{\in \mathcal{A}(M)} + m_1 \otimes m_2 + m_2 \otimes m_1 + \underbrace{m_2 \otimes m_2}_{\in \mathcal{A}(M)} \implies m_1 \otimes m_2 + m_2 \otimes m_1 \in \mathcal{A}(M)$$

Therefore, $m_1 \wedge m_2 = -m_2 \wedge m_1$.

Question 4.84. *Can we go from $m_1 \otimes m_2 + m_2 \otimes m_1 \in \mathcal{A}(M)$ to $m \otimes m$? Not always! If we let $m_1 = m_2 = m$, then we get $2m \otimes m \in \mathcal{A}(M)$, which fails if the characteristic of R is even. We would need 2 to be a unit in R. This would then make our definition sloppy!*

Recall, for $\sigma \in \mathcal{S}_k, (-1)^\sigma = \epsilon(\sigma) = sign(\sigma)$. Clearly, $sign(i \cdot (i+1)) = -1$. Moreover, $(-1)^{odd} = -1$ and $(-1)^{even} = +1$.

Theorem 4.85. *1. $\bigwedge^k(M) = \mathcal{T}^k(M)/\mathcal{A}^k(M)$ and $\mathcal{A}^k(M) = \langle m_1 \otimes m_2 \otimes \ldots \otimes m_k : m_i = m_j \text{ for some } i \neq j \rangle$*

2. (Universal property for alternating k-multilinear maps) If $\phi : M \times M \times \ldots \times M \to N$ is an alternating k-multilinear map then there is a unique R-module homomorphism $\Phi : \bigwedge^k(M) \to N$ such that $\phi = \Phi \circ i$, where
$$i : M \times \ldots \times M \to \bigwedge^k(M)$$
$$i(m_1, \ldots, m_k) = m_1 \wedge \ldots \wedge m_k$$

3. *(Universal Property for R-algebras) For any R-algebras A with $a^2 = 0$ for all $a \in A$, and given an R-module homomorphism $\phi : M \to A$, there exists an R-algebra homomorphism $\Phi : \bigwedge(M) \to A$*

Example 4.86. *Let $R = \mathbb{F}$ and $M = V \cong \mathbb{F}^n$ an n-dimensional vector space with basis $\{v_1, \ldots, v_n\}$. Then we see that*

- $\bigwedge^1(V) = \mathbb{F}$
- $\bigwedge^1(V) = V$
- *To see $\bigwedge^2(V)$, we notice the calculation*

$$\sum_i a_i v_i \wedge \sum_j b_j v_j = \sum_{i,j} a_i b_j (v_i \wedge v_j) = \sum_{i \leq j} (a_i b_j - a_j b_i)(v_i \wedge v_j) = \sum_{i<j} (a_i b_j - a_j b_i)(v_i \wedge v_j)$$

  So $\bigwedge^2(V) = span\{v_i \wedge v_j : 1 \leq i < j \leq n\}$ and has dimension $\binom{n}{2}$.
- *In general, $dim_{\mathbb{F}} \bigwedge^k(V) = \binom{n}{k}$ with $\bigwedge^n(V) = span\{v_1 \wedge v_2 \wedge \ldots \wedge v_n\}$*
- $\bigwedge^{n+1}(V) = 0$

Therefore, we see that

$$\bigwedge(V) = \mathbb{F} \oplus V \oplus \overset{2}{\bigwedge}(M) \oplus \ldots \oplus \overset{n}{\bigwedge}(V)$$

Remark 4.87. *For R commutative, and M a free R-module of rank n, this example extends very nicely in which each $\bigwedge^k(M)$ is free with similar basis for $1 \leq k \leq n$ and then we have this cancelation for $\bigwedge^{>n}(M) = 0$.*

Example 4.88. *Let $R = \mathbb{Z}, M = \mathbb{Q},$, then*

$$\bigwedge(M) = \mathbb{Z} \oplus \mathbb{Q}$$

since $1 \oplus 1 = 0$ and any simple tensor in $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ is $a \cdot 1 \otimes 1$.

4.6 Induced Homomorphisms between Algebras

Let R be a commutative ring, with modules ${}_RM, {}_RN$. Let $\phi \in Hom_R(M, N)$. Then we get an induced homomorphism of the graded rings $\mathcal{T}(\phi) : \mathcal{T}(M) \to \mathcal{T}(N)$ and the R-module maps $\mathcal{T}^k(\phi) : \mathcal{T}^k(M) \to \mathcal{T}^k(N)$ via

$$m_1 \otimes m_2 \otimes \ldots \otimes m_k \to \phi(m_1) \otimes \phi(m_2) \otimes \ldots \otimes \phi(m_k)$$

Further, we see that since $\mathcal{T}(\phi)[\mathcal{C}(M)] \subset \mathcal{C}(N)$ and $\mathcal{T}(\phi)[\mathcal{A}(M)] \subset \mathcal{A}(N)$, then we also get the induced homomorphisms:

$$\mathcal{S}(\phi) : \mathcal{S}(M) \to \mathcal{S}(N) \qquad \mathcal{S}^k(\phi) : \mathcal{S}^k(M) \to \mathcal{S}^k(N)$$

$$\bigwedge(\phi) : \bigwedge(M) \to \bigwedge(N) \qquad \overset{k}{\bigwedge}(\phi) : \overset{k}{\bigwedge}(M) \to \overset{k}{\bigwedge}(N)$$

Example 4.89. *Let $R = \mathbb{R}, M = V = N$ where $V = \mathbb{F}^n$, an n-dimensional vector space with basis $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$. Exploring these implications by dimension, we can initially recall $dim_{\mathbb{F}}(\bigwedge^n V) = 1$. But what is the map*

$$\overset{n}{\bigwedge}(\phi) : \overset{n}{\bigwedge}(V) \to \overset{n}{\bigwedge}(V)?$$

It must be a scalar! If $n = 2$, then if $\phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with respect to basis $\mathcal{B}$, then

$$\begin{aligned} \overset{2}{\bigwedge}(\phi) : v_1 \wedge v_2 &\to (av_1 + cv_2) \wedge (bv_1 + dv_2) \\ &= abv_1 \wedge v_1 asv_1 \wedge v_2 + bcv_2 \wedge v_1 + cdv_2 \wedge v_2 \\ &= (as - bc)v_1 \wedge v_2 \\ &= D(\phi)v_1 \wedge v_2 \end{aligned}$$

Here, $D(\phi)$ is known as the <u>determinant</u> of ϕ.

Remark 4.90. *ϕ can be injective, but it's induced homomorphisms in $\mathcal{S}^k(\phi), \bigwedge^k(\phi)$ need not be injective.*

Example 4.91. *Let $R = \mathbb{Z}[x, y], N = R, M = I = \langle x, y\rangle$. Then $\bigwedge^2(R) = 0$ but $\bigwedge^2(I) \neq 0$. Here I is a homogenous graded ideal.*

4.7 Symmetric and Alternating Tensors

Theorem 4.92. *$\mathcal{T}^k(M)$ is a left $R[\mathcal{S}^k]$-module with $\sigma \in \mathcal{S}_k$ action defined on a simple tensor by*

$$\sigma \cdot m_1 \otimes m_2 \otimes \ldots \otimes m_k = m_{\sigma^{-1}(1)} \otimes m_{\sigma^{-1}(2)} \otimes \ldots \otimes m_{\sigma^{-1}(k)}$$

Remark 4.93. *Warning: $m_{\sigma(1)} \otimes m_{\sigma(2)} \otimes \ldots \otimes m_{\sigma(k)}$ is a RIGHT action. This is related to the permutation matrix $P(\sigma) : e_i \to e_{\sigma(i)}$ has $P(\sigma)P(\tau) = P(\sigma\tau)$. Then*

$$P(\sigma) \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} a_{\sigma^{-1}(1)} \\ a_{\sigma^{-1}(2)} \\ \vdots \\ a_{\sigma^{-1}(k)} \end{pmatrix}$$

Example 4.94. $s_1 s_2 = (1\ 2)(2\ 3) = (1\ 2\ 3)$. *But notice,*

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} a_3 \\ a_1 \\ a_2 \end{pmatrix}$$

Definition 4.95. *For any $z \in \mathcal{T}^k(M)$ is a <u>symmetric k-tensor</u> if $\sigma \cdot z = z$ for all $\sigma \in \mathcal{S}_k$. This need not be a simple tensor.*

Definition 4.96. *For any $z \in \mathcal{T}^k(M)$ is an <u>alternating k-tensor</u> if $\sigma \cdot z = (-1)^\sigma z$ for all $\sigma \in \mathcal{S}_k$.*

Example 4.97. *$m_1 \otimes m_1, m_1 \otimes m_2 + m_2 \otimes m_1 \in \mathcal{T}^2(M)$ are symmetric 2-tensors and $m_1 \otimes m_2 - m_2 \otimes m_1$ is an alternating 2-tensor.*

Note 4.98. *$\mathcal{C}^k(M)$ and $\mathcal{A}^k(M)$ are $R[\mathcal{S}_k]$-submodules of $\mathcal{T}^k(M)$. So $\mathcal{S}^k(M), \bigwedge^k(M)$ are $R[\mathcal{S}_k]$-modules.*

Proposition 4.99. *With these induced actions:*

1. *For all $v \in \mathcal{S}^k(M), \sigma \cdot v = v$ for all $\sigma \in \mathcal{S}_k$.*
2. *For all $v \in \bigwedge^k(M), \sigma \cdot v = (-1)^\sigma v$ for all $\sigma \in \mathcal{S}_k$.*

Proof. Define the sums:

$$Sym := \sum_{\sigma \in \mathcal{S}_k} \sigma$$

$$Alt := \sum_{\sigma \in \mathcal{S}_k} (-1)^\sigma \sigma$$

Then $\sigma Sym = Sym$ and $\sigma Alt = (-1)^\sigma Alt$ for all $\sigma \in \mathcal{S}_k$. So

$$Sym \cdot Sym = k! Sym \qquad Alt \cdot Alt = k! Alt$$

In $\mathcal{Q}[\mathcal{S}_k]$, (or R in which $k! \in R^\times$, we can identify the idempotents:

$$e_{triv} = \frac{1}{k!} Sym \qquad e_{sgn} = \frac{1}{k!} Alt$$

Then we see that $e_{triv}^2 = e_{triv}, e_{sgn}^2 = e_{sgn}$. Then we see that given $z \in \mathcal{T}^k(M)$ then we see that, we can define

$$Sym \cdot z := \text{ the symmetrization of } z$$

$$Alt \cdot z := \text{ the skew-symmetrization of } z$$

- If z is a symmetric k-tensor, then

$$e_{triv}z = z \qquad e_{sgn}z = 0$$
$$Sym \cdot z = k!z \qquad Alt \cdot z = 0$$

- If z is an alternating k-tensor, then

$$e_{triv}z = 0 \qquad e_{sgn}z = z$$
$$Sym \cdot z = 0 \qquad Alt \cdot z = k!z$$

■

Proposition 4.100. *Suppose $k!$ is a unit in R. Clearly e_{triv}, e_{sgn} are the idempotents of the group ring $R[\mathcal{S}_k]$. Moreover,*

1. *Consider the map*

$$\phi : \mathcal{T}^k(M) \to \mathcal{T}^k(M)$$
$$z \to e_{triv}z$$

Then

- *$Im\phi :=$ R-submodule of the symmetric k-tensors in $\mathcal{T}^k(M)$*
- *$Ker(\phi) = \mathcal{C}^k(M)$*

And so, ϕ serves as an isomorphism between $\mathcal{S}^k(M) \cong$ symmetric k-tensors as R-module OR $R[\mathcal{S}_k]$-modules.

2. *Consider the map*

$$\psi : \mathcal{T}^k(M) \to \mathcal{T}^k(M)$$
$$z \to e_{sgn}z$$

Then

- *$Im\phi :=$ R-submodule of the alternating k-tensors in $\mathcal{T}^k(M)$*
- *$Ker(\phi) = \mathcal{A}^k(M)$*

And so, ψ serves as an isomorphism between $\bigwedge^k(M) \cong$ alternating k-tensors as R-module OR $R[\mathcal{S}_k]$-modules.

Proof. 1. It is easy to see that $\mathcal{C}^k(M) \subset Ker(\phi)$. That is,

$$e_{triv}(z - \sigma z) = e_{triv}z - e_{triv}z = 0$$

If $0 = \phi(z) = e_{triv}$, then

$$z = z - e_{triv}z = \frac{1}{k!}\left[\sum_{\sigma \in \mathcal{S}_k}(z - \sigma z)\right] \in \mathcal{C}^k(M)$$

Also, $Im(\phi) =$ { symmetric k-tensors } since $\sigma e_{triv} = e_{triv} \implies Im(\phi) \subset$ { symmetric k-tensors }. For the other direction, we know that if z is symmetric, then $e_{triv}z = z$. So

$$\frac{1}{k!}\sum_{\sigma \in \mathcal{S}_k}\sigma \cdot z = \frac{1}{k!}\sum_{\sigma \in \mathcal{S}_k} z = z$$

2. The proof of (2) is similar to (1).

■

Note 4.101. *Alternatively, one could restrict the domain of ϕ to the symmetric k-tensors and compose with $\mathcal{T}^k(M) \xrightarrow{\pi} \mathcal{S}^k(M)$. This will also be an isomorphism!*

Note 4.102. *$\mathcal{C}(M)$ is the ideal generated by $m_1 \otimes m_2 - m_2 \otimes m_1$. Notice, $\mathcal{C}^k(M)$ is generated as an R-module by $Alt \cdot (m_1 \otimes m_2 \otimes \ldots \otimes m_k)$.*

Note 4.103. *Because e_{triv}, e_{sgn} are idempotents and ϕ, ψ are projection, then we see that*

$$\mathcal{T}^k(M) \cong Ker\phi \oplus Im\phi = \mathcal{C}^k(M) \oplus \mathcal{S}^k(M)$$

$$\mathcal{T}^k(M) \cong Ker\psi \oplus Im\psi = \mathcal{A}^k(M) \oplus \bigwedge^k(M)$$

So even though $\mathcal{S}^k(M)$ is a quotient, we can realize it as a submodule via ϕ with complement $\mathcal{C}^k(M)$. The same can be said about $\bigwedge^k(M)$ with complement $\mathcal{A}^k(M)$.

Note 4.104. *$\mathbb{C}[\mathcal{S}_k]$ has other central idempotents. We can look at similar projections for $\mathcal{T}^k(V)$ where $R = \mathbb{C}, V = \mathbb{C}^n$, which is an $GL_n(\mathbb{C})$-module. This is an example of Schur-Weyl Duality.*

5 More on Modules

5.1 Jordan-Hölder Theorem for Modules

Definition 5.1. *A filtration ending in $\{0\}$ (or series) of a left R-module M is the of submodules*

$$M = M_0 \supset M_1 \supset \ldots \supset M_n = \{0\}$$

We call M_i/M_{i+1} the factor modules, and the number of strict inclusions is the length of the filtration.

Example 5.2. *Let $R = \mathbb{Z}, M = \mathbb{Z}/4\mathbb{Z}$. Then*

$$\mathbb{Z}/4\mathbb{Z} \supset 2\mathbb{Z}/4\mathbb{Z} \supset 4\mathbb{Z}/4\mathbb{Z} = \{0\}$$

which has length 2 and the factor modules are $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$ by the 3rd isomorphism theorem.

Example 5.3. *Let $R = \mathbb{Z}, N = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then*

$$N \supset \mathbb{Z}/2\mathbb{Z} \times \{\bar{0}\} \supset \{(\bar{0}, \bar{0})\}$$

has length 2 with factor modules $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$. We could have also take the series to be

$$N \supset \{\bar{0}\} \times \mathbb{Z}/2\mathbb{Z} \supset \{(\bar{0}, \bar{0})\}$$

which have the same factor modules.

Example 5.4. *$\mathbb{Z}/4\mathbb{Z} \subset \{0\}$ is also a filtration of length 1.*

Example 5.5. *$\mathbb{Z} \supset 2\mathbb{Z} \supset 8\mathbb{Z} \supset 56\mathbb{Z} \supset \{0\}$ has length 4, and the repetition of improper inclusions still leaves us with length 4: $\mathbb{Z} \supset 2\mathbb{Z} \supset 2\mathbb{Z} \supset 8\mathbb{Z} \supset 56\mathbb{Z} \supset \{0\}$.*

Note 5.6. *Sometimes we see the notation $M_\bullet$ for series or $\mathcal{F}^\bullet$ and instead write $M_i = \mathcal{F}^i M$*

Definition 5.7. *A refinement of a series $M = M_0 \supset M_1 \supset \ldots \supset M_k = \{0\}$ is a series $M = M_0' \supset M_1' \supset \ldots \supset M_t' = \{0\}$ which has the M_i as a subsequence. That is, each M_i occurs as M_j' for some j.*

Definition 5.8. *Two series of M are equivalent if their nonzero factor modules are in bijection and isomorphic.*

Example 5.9. *The series*

$$\mathbb{Z} \supset 3\mathbb{Z} \supset 6\mathbb{Z} \supset 12\mathbb{Z} \supset \{0\}$$

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 6\mathbb{Z} \supset 12\mathbb{Z} \supset \{0\}$$

both of which have factors

$$\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \text{ and } 12\mathbb{Z}$$

though not in the same order.

Theorem 5.10 (Schreier Refinement Theorem)**.** *Any two series of M have equivalent refinements!*

Definition 5.11. *A composition series of a module ${}_RM$ is a series whose nonzero factor modules are all simple R-modules.*

Remark 5.12. *$R = \mathbb{Z}, M = \mathbb{Z}$ has no composition series.*

Theorem 5.13 (Jordan-Hödler for Modules)**.** *Any two composition series of ${}_RM$ are equivalent. In particular, they have the same length.*

Proof. Jordan-Hölder follows from Schreier refinement since any refinement of a composition series is equivalent to the original series. That is M_1/M_2 simple $\iff M_2 \subset M_1$ is maximal. ■

Definition 5.14. *If ${}_RM$ has a composition series, its length is called the length of M.*

Definition 5.15. *Letting $R = \mathbb{Z}, M = \mathbb{Z}/4\mathbb{Z}$ has length 2.*

Corollary 5.15.1. *If M has the ascending chain condition or the descending chain condition on submodules, then M has finite length.*

Now, in order to prove the Schreier Refinement Theorem, we need a lemma known as the Butterfly Lemma

Lemma 5.16. *Given $A \subset A^* \subset M$ and $B \subset B^* \subset M$, then*

$$[A + (A^* \cap B^)]/[A + (A^* \cap B)] \cong [B + (A^* \cap B^)]/[B + (A \cap B^*)]$$

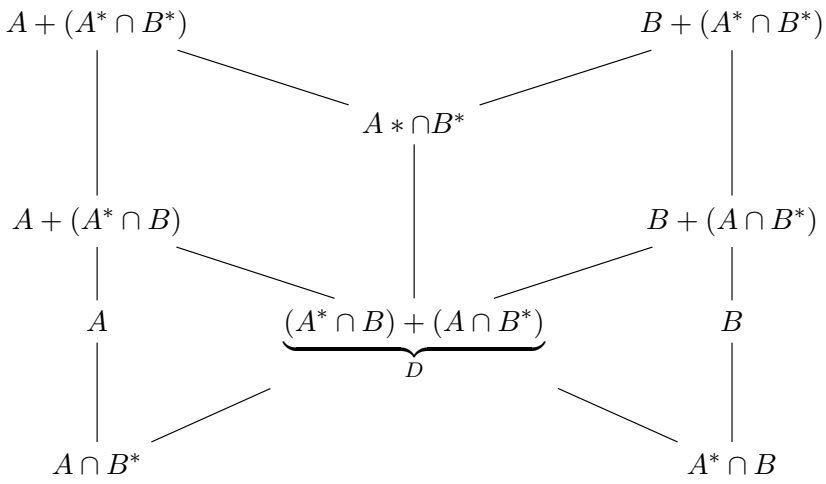
Example 5.17. *Observe, $A = 12\mathbb{Z} \subset A^* = 4\mathbb{Z} \subset \mathbb{Z}$ and $B = 18\mathbb{Z} \subset B^* = 6\mathbb{Z} \subset \mathbb{Z}$. Then we see that*

$$[12\mathbb{Z} + (4\mathbb{Z} \cap 6\mathbb{Z})]/[12\mathbb{Z} + (4\mathbb{Z} \cap 18\mathbb{Z})] \cong [12\mathbb{Z} + 12\mathbb{Z}]/[12\mathbb{Z} + 36\mathbb{Z}] = 12\mathbb{Z}/12\mathbb{Z} = \{0\}$$

$$[18\mathbb{Z} + (4\mathbb{Z} \cap 6\mathbb{Z})]/[18\mathbb{Z} + (12\mathbb{Z} \cap 6\mathbb{Z})] \cong [18\mathbb{Z} + 12\mathbb{Z}]/[18\mathbb{Z} + 12\mathbb{Z}] = 6\mathbb{Z}/6\mathbb{Z} = \{0\}$$

Notice, we get the same answer!

Proof. (Of Lemma)
We see that we can construct the the following diagram:



So we can show leverage the A-B symmetry and simple demonstrate that

$$[A + (A^* \cap B^*)]/[A + (A^* \cap B)] \cong A^* \cap B^*/D$$

To do so, we consider the mapping:

$$\phi : A + (A^* \cap B^*) \to A^* \cap B^*/D$$
$$a + x \to x + D$$

- ϕ is well-defined: If $a + x = a' + x'$ for some $a, a' \in A, x, x' \in A^* \cap B^*$, then we see that

  $$a - a' = x' - x \in A \cap (A^* \cap B^*) = A \cap B^* \subset (A^* \cap B) + (A \cap B^*) = D$$

  So $x + D = x' + D$.

- ϕ is an R-module homomorphism: Left as an exercise.

- To identify $Ker(\phi)$, observe if $\phi(a + x) = 0 + D \implies x \in D$. So $a + x \subset A + D = A + (A^* \cap B)$. If $a + x \in A + (A^* \cap B)$, then by the well-definedness of our mapping, we know $x \in A^* \cap B \subset D$. So

  $$Ker(\phi) = A + (A^* \cap B)$$

- To identify $Im(\phi)$, we notice that since $A^* \cap B^* \subset A + (A^* \cap B^*)$, then ϕ is surjective.

Therefore, by the First Isomorphism Theorem, we see

$$[A + (A^* \cap B^*)]/[A + (A^* \cap B)] \cong A^* \cap B^*/D$$

■

Proof. (Of Schreier Refinement Theorem)
Suppose

$$M = A_0 \supset A_1 \supset \ldots \supset A_n = \{0\}$$
$$M = B_0 \supset B_1 \supset \ldots \supset B_k = \{0\}$$

are two series of M. We can refine each series by

- For the first series, squeezing in between each pairs of the first series, k terms: For $0 \leq i < n$,

  $$A_{ij} = A_{i+1} + (A_i \cap B_j)$$

  Then we see

  $$A_i = A_{i0} \supset A_{i1} \supset \ldots \supset A_{1k} = A_{i+1}$$

  So we arrive at the refinement

  $$M = A_{0,0} \supset A_{0,1} \supset \ldots \supset A_{0,k} = A_{1,0} \supset A_{1,1} \supset \ldots \supset A_{n-1,0} = A_{n-1,1} \supset \ldots \supset A_{n-1,k} = \{0\}$$

- Similarly, for the second series, we refine:

  $$M = B_{0,0} \supset B_{0,1} \supset \ldots \supset B_{0,n} = B_{1,0} \supset B_{1,1} \supset \ldots \supset B_{k-1,0} = A_{k-1,1} \supset \ldots \supset B_{k-1,n} = \{0\}$$

Now, if we collapse the $A_{i,k} = A_{i+1,0}$ and $B_{j,n} = B_{j+1,0}$, then we see each series has exactly nk length. To check the composition factors, we use the Zassenhaus / Butterfly lemma to see

$$A_{i,j}/A_{i,j+1} = [A_{i+1} + (A_i^* + B_j^*)]/[A_{i+1} + (A_i^* + B_{j+1})]$$
$$B_{j,i}/A_{j,i+1} = [B_{j+1} + (B_j^* \cap A_i^*)]/[B_{j+1} + (B_j^* + A_{i+1})]$$

Therefore, we see that all of the factors are shared between each of the series. So we have shown that both series are equivalent! ■

5.2 Finitely Generated Modules of a PID

Example 5.18. *Let $R = \mathbb{Z}$. A finitely generated $\mathbb{Z}$-modules M is isomorphic to*

$$M \cong \underbrace{\mathbb{Z}^r}_{free} \oplus \underbrace{T}_{torsion/finite}$$

A finite $\mathbb{Z}$-module T is isomorphic to

$$\mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/a_2\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_m\mathbb{Z}$$

where $a_i | a_{i+1} \iff \langle a_i \rangle \supset \langle a_{i+1} \rangle$ and $a_i \neq 0$.
If $T \neq \{0\}$, then we have $a_1 > 1$, and if we take all $a_i > 1$, then the a_i are unique. So m is an invariant, called the invariant factor form and the $\{a_i\}$ are called the invariant factors.

Example 5.19. *$T = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/50\mathbb{Z}$. This is a "maximal clumping" under the Chinese Remainder Theorem. If you do "minimal clumping", we get elementary divisors.*

$$T = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/50\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/25\mathbb{Z}$$

So you can decompose T into $\oplus p$ primary components, which are the summands with p^N for some $N >> 0$. But each p-primary component might or might not decompose further.

Proposition 5.20. *Let R be an integral domain. Let M be a free R-module of rank $n < \infty$. Then any set of $n+1$ elements $y_i \in M$ satisfy some R-linear dependent relation. That is, there exists $r_1, \ldots, r_{n+1}$ not all zero such that*

$$r_1 y_1 + \ldots r_{n+1} y_{n+1} = 0$$

Proof. Let F be the field of fractions of R, and think of $R \subset F$ as a subring. We can embed

$$M = \bigoplus_{i=1}^{n} R \subset \bigoplus_{i=1}^{n} F$$

Then $\{y_i\}_{i=1}^{n+1}$ are F-linearly dependent. We can write a relation

$$a_1 y_1 + \ldots + a_{n+1} y_{n+1} = 0$$

with $a_i \in F$ and at least one $a_i \neq 0$. But if we clear the denominators of each a_i, we get a relation with coefficients in R. Since R is a domain, then we will retain that $r_i \neq 0$. ■

Definition 5.21. $\underline{Tor(M) :=} \{x \in M : rx = 0 \text{ for some } r \in R \setminus \{0\}\}$.

In the homework, you showed this in an R-module of M when R is an integral domain. Any submodule $N \subset Tor(M) \subset M$ is called a <u>torsion submodule</u> of M.

Definition 5.22. $\underline{Ann(N) :=} \{r \in R : rn = 0 \ \ \forall n \in N\}$.

Exercise 5.23. *Show that $Ann(N) \subset R$ is a 2-sided ideal.*

Exercise 5.24. *For any $N \subset L \implies Ann(N) \supset Ann(L)$. If R is a PID, we can rewrite this by principal ideal $\langle b \rangle \supset \langle a \rangle$.*

Exercise 5.25. *If R is an integral domain, and if N is <u>not</u> torsion, then $Ann(N) = \{0\}$.*

Definition 5.26. *Let R be an integral domain and M be an R-module. The <u>fake rank</u> of M is the maximal size of a subset of R-linearly independent elements of M.*

Proposition 5.27. *If M is a free R-module, then the rank of M is equal to the fake rank of M. So these definitions are consistent for free modules.*

Proof. If $M = \bigoplus_{i=1}^{n} R$ is free of rank n and F is the field of fractions of R. Then

$$F \otimes_R M \cong \bigoplus_{i=1}^{n} F$$

■

Proposition 5.28. *If N is torsion, then $F \otimes_R N = 0$.*

Proof. If $n \in N$, then there exists $r \in R$ such that $r \neq 0$, $rn = 0$. Then we see

$$1 \otimes n = r^{-1} r \otimes n = r^{-1} \otimes rn = r^{-1} \otimes 0 = 1 \otimes 0 = 0$$

Notice, any such n cannot belong to a set of R-linearly independent elements. ■

Proposition 5.29. *The fake rank of M is $dim_F(F \otimes_R M)$.*

Theorem 5.30. *Let R be a PID. Let M be a free R-module of rank n, with $N \subset M$ a submodule. Then*

1. *N is also free. The rank of N is less than n.*
2. *There exists a basis $\{y_1, y_2, \ldots, y_n\}$ of M such that $\{a_1 y_1, a_2 y_2, \ldots, a_m y_m\}$ is a basis of N with $a_i \in R \setminus \{0\}$ and $a_i | a_{i+1}$, which is the same as saying $\langle a_i \rangle \supset \langle a_{i+1} \rangle$.*

Proof. If $N = \{0\}$, then we take $\emptyset$ to be the subset from the basis of M. So the theorem holds for the trivial case. Now, assume $N \neq \{0\}$. Define

$$\Sigma := \{\langle a_\phi \rangle : \phi \in Hom_R(M, R), \phi(N) = \langle a_\phi \rangle\}$$

Clearly, $\langle 0 \rangle \in \Sigma \implies \Sigma$ is nonempty.

In previous lecture, we showed that a PID is Noetherian with the ascending chain condition on ideals. So a nonempty collection of ideals has a maximal element. So we let

$$\langle a_\nu \rangle$$

be the maximal element of Σ. So $\langle a_\nu \rangle = \nu(N) \subset R$. Let $a_1 = a_\nu$ and $y \in N$ be such that $\nu(y) = a_1$.

First, we claim $a_1 \neq 0$. Suppose otherwise. Then $\langle 0 \rangle \in \Sigma$ was a maximal element, which would mean $\Sigma = \{\langle 0 \rangle\}$. So for any $\phi : M \to R, \phi(N) = 0$. Now let $\{x_1, \ldots, x_n\}$ be the basis of M. Since $N \neq 0$, there exists some $\sum_i s_i x_i = n' \in N$. So for some i, $s_i \in R$ cannot be zero. Now construct the mapping

$$\pi_i : M \to R$$
$$\sum_{j=1}^{n} c_j x_j \to c_i$$

Then $0 \neq s_i = \pi_i(n') \in \pi_i(N)$. But this contradicts what was stated that $\phi(N) = 0$.
Second, to account for the divisibility, we let $a_1 = a_\nu = \nu(y)$ divides $\phi(y)$ for all $\phi \in Hom_R(M, R)$. That is, $\langle \phi(y) \rangle \subset \langle a_1 \rangle$. Let $\langle d \rangle = \langle a_1 \rangle + \langle \phi(y) \rangle = \langle \nu(y) \rangle + \langle \phi(y) \rangle$. Then we can write

$$d = r_1 \nu(y) + r_2 \phi(y)$$

for some $r_1, r_2 \in R$. Let

$$\psi := r_1 \nu + r_2 \phi \in Hom_R(M, R)$$

Notice, $\psi(y) = d$. So

$$\langle a_1 \rangle \subset \langle d \rangle = \langle \psi(y) \rangle \subset \langle a_\psi \rangle$$

since $y \in N$, so $\psi(y) \in \psi(N)$. By maximality, then we know

$$\langle a_1 \rangle = \langle d \rangle = \langle \psi(y) \rangle = \langle a_\psi \rangle$$

So we see $\langle \phi(y) \rangle \subset \langle a_1 \rangle$.
This $\pi_j(y) \in \langle a_1 \rangle$ for $1 \leq j \leq n$. We can write $\pi_i(y) = a_1 b_j$, for some $b_j \in R$. Now, define

$$y_1 := \sum_{j=1}^{n} b_j x_j$$

Observe, $a_1 = a_\nu = \nu(y) = \nu\left(\sum_{j=1}^n a_1 b_j x_j\right) = a_1 \nu\left(\sum_{j=1}^n b_j x_j\right) = a_1 \nu(y_1)$ So $1 = \nu(y_1)$ since $a_1 \neq 0$, and R is a PID!
Next, we want to extent $\langle y_1 \rangle$ to a basis of M and $\langle a_1 y_1 \rangle$ to a basis of N. To do so, we use induction.

1. Want to show $M = Ry_1 \oplus Ker(\nu)$. Let $x \in M$. We can write

   $$x = \nu(x) y_1 + (x - \nu(x) y_1)$$

   where $\nu(x) y_1 \in Ry_1$. So

   $$\nu[x - \nu(x) y_1] = \nu(x) - \nu(\nu(x) y_1) = \nu(x) - \nu(x)\nu(y_1) = \nu(x) - \nu(x) 1 = 0$$

   So $x - \nu(x) y_1 \in Ker(\nu)$. So $M = Ry_1 + Ker(\nu)$. To check the intersection, we see that if $ry_1 \in Ker(\nu)$, then

   $$0 = \nu(ry_1) = r\nu(y_1) = r \cdot 1 = r$$

   So $ry_1 = 0$.

2. Let $N = Ra_1y_1 \oplus (N \cap Ker(\nu))$. Let $x' \in N$. Recall $a_1 = a_\nu$ such that $\langle a_\nu \rangle = \langle \nu(N) \rangle$. So $\langle a_1 \rangle \supset \langle \nu(x') \rangle$. We can write $ba_1 = \nu(x')$, and

$$x' = \nu(x)y_1 + (x' - \nu(x')y_1) = \underbrace{ba_1y_1}_{Ra_1y_1} + \underbrace{(x' - ba_1y_1)}_{\in N}$$

Since $Ry_1 \cap Ker(\nu) = \{0\}$, then we also see that

$$Ra_1y_1 \cap (N \cap Ker(\nu)) = \{0\}$$

Taking these two arguments, we can induct on $m =$ fake rank of $N \subset M$ the free module of rank n. Observe:

- $m = 0, \implies N$ is torsion! But $Tor(M) = 0$ since M is free, so $N = 0$.
- Let $m > 0$. By (1), we know
$$N = Ra_1y_1 \oplus (N \cap Ker(\nu))$$
the let the fake rank of $N \cap Ker(\nu)$ to be $m - 1$. If we take $a_n y^m z_j \in N \cap Ker(\nu)$, then $a_1y_1 \cup \{z_j\}_{j=1}^m \subset N$ has an R-dependence relation
$$c_0a_1y_1 + \sum_{j=1}^m c_jz_j = 0$$
where $c_j \in R$. But by the direct sum, we know
$$\sum_{j=1}^m c_jz_j = 0$$
So we fake rank $N \cap Ker(\nu) \leq m - 1$. We can show the opposite direction, but in this context, it follows from below.

Now, by induction, $N \cap Ker(\nu)$ is free of rank $k \leq m - 1$. Thus it has a basis $\{w_1, \ldots, w_k\}$. Then $\{a_1y_1, w_1, \ldots, w_k\}$ is a basis of
$$N = Ra_1y_1 \oplus (N \cap Ker(\nu))$$
The directness shows that any $v \in N$ can be written
$$v = c_0a_1y_1 + \sum_{j=1}^k c_jw_j$$
and this spanning set being a basis provides uniqueness, and hence R-independence. Thus N is free of rank $k + 1$.

Therefore we see that this rank must agree with the fake rank! So $k = m - 1$. So N is free of rank m.

To prove the second statement, we already have a_1, y_1. We can now induct on $n = rank(M)$. By (1), $Ker(\nu) \subset M$ is free and recall $M = Ry_1 \oplus Ker(\nu)$. So as before, $Ker(\nu)$ is free of rank $n - 1$. By induction, $N \cap Ker(\nu) \subset Ker(\nu)$ is free so by the inductive hypothesis, $Ker(\nu)$ has some basis $\{y_2, \ldots, y_n\}$ such that $\{a_2y_2, \ldots, a_my_m\}$ is a basis of $N \cap Ker(\nu)$ and further, $a_j | a_{j+1}$ for $j \geq 2, a_j \in R$.

Using the direct sums in (1),(2), we know $\{y_1, \ldots, y_n\}$ is a basis of M, and $\{a_1y_1, a_2y_2, \ldots, a_my_m\}$ is a basis of N. All we need to be done is to show that $a_1 | a_2$.

Define the mapping $\phi \in Hom_R(M, R)$ by $\phi(y_1) = \phi(y_2) = 1, \phi(y_i) = 0$ for $i > 2$. Notice, $\phi(a_1y_1) = a, \phi(a_2y_2) = a_2$. So we simply need to show that $\langle \phi(N) \rangle \supset \langle a_1 \rangle$ and $\langle \phi(N) \rangle \supset \langle a_2 \rangle$. But by maximality in Σ, we know
$$\langle \phi(N) \rangle = \langle a_1 \rangle \supset \langle a_2 \rangle$$

■

Example 5.31. *Consider $M = \mathbb{Z} \oplus \mathbb{Z}$ a $\mathbb{Z}$-module with the basis $\{(1,1)\}$. Then $N = \{(x,x) : x \in \mathbb{Z}\}$ is also a free $\mathbb{Z}$-submodule but $O = \{(x,0) : x \in \mathbb{Z}\}$ is NOT a free $\mathbb{Z}$-submodule.*

Example 5.32. *(Nonexample) $R = \mathbb{Z}[x]$ with $\langle x, 2\rangle \subset R$. Here R is a free R-module, yet R is not a PID. Then the theorem doesn't apply. In particular, $\langle x, 2\rangle \subset R$ is not a free module.*

Example 5.33. *Let $M = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ over the ring $R = \mathbb{Z}$. Let $N \subset M$ be some submodule. N is finitely generated, since $\mathbb{Z}$ is a PID $\implies$ Noetherian $\implies$ M if finitely generated $\implies$ all submodules are finitely generated. Say, N is generated as a $\mathbb{Z}$-module by*

$$\langle (1,2,3), (-1,0,1), (1,1,1)\rangle$$

First, is $N = M$? If so, this would be a basis. Recall, the columns of the elements of $GL_n(\mathbb{Z})$ are bases of M! So we can put these vectors in a matrix:

$$\begin{pmatrix} 1 & -1 & 1 \\ 2 & 0 & 1 \\ 3 & 1 & 1 \end{pmatrix}$$

and calculate the determinant. You can also try and identify the basis by one of two methods:

- *Row reduction preserves the span of rows.*
- *Column reduction preserve the span of the columns.*

So taking the form of the matrix that is convenient, we perform row reduction:

$$\begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 4 \\ 0 & -1 & -2 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \\ 0 & 2 & 4 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

Therefore, $N = \langle (1,0,-1), (0,1,2)\rangle$. Moreover, we can complete the basis

$$\{(1,0,-1), (0,1,2), (0,0,1)\}$$

of $\mathbb{Z}^3$, and have $a_1 = 1, a_2 = 1$.
On the other hand, what about the submodule $L = \langle (1,2,3), (-1,0,1)\rangle$. Then we get

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 4 \end{pmatrix}$$

So we have $a_1 = 1, a_2 = 2$. What if we have

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 1 \end{pmatrix}$$

Then we can actually complete to a basis:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

but this is pretty ad hoc. We can consider a better way to go about this.

Example 5.34. *Let $M \subset \mathbb{Z}^3$ generated by the elements :*

$$\{(3,-9,12), (6,-18,6), (9,-27,42)\}$$

Find a basis $\{y_1, y_2, y_3\}$ of $\mathbb{Z}^3$ so if M has rank m, the basis of M is $\{a_1 y_1, \ldots, a_n y_m\}$ such that $a_1 | a_2, \ldots$. First, put vectors into rows:

$$\begin{pmatrix} 3 & -9 & 12 \\ 6 & -18 & -6 \\ 9 & -27 & 42 \end{pmatrix}$$

So we can row reduce AND column reduce in order to yield a diagonal matrix:

$$D = \begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & * \end{pmatrix} = PAQ^{-1}$$

where $P, Q \in GL_3(\mathbb{Z})$.
Row reduction and column reduction can actually be equated to a left or right matrix multiplication action:

$$R_i \to R_i + a_{i,j}R_j \iff \textit{left multiplication by } E_{i,j}(a) = \begin{pmatrix} 1 & & a \\ & 1 & \\ & & 1 \end{pmatrix} \textit{ or } \begin{pmatrix} 1 & & \\ a & 1 & \\ & & 1 \end{pmatrix} \in GL_n(\mathbb{Z})$$

$$C_j \to C_j + a_{i,j}C_i \iff \textit{right multiplication by } E_{i,j}(a) = \begin{pmatrix} 1 & & a \\ & 1 & \\ & & 1 \end{pmatrix} \textit{ or } \begin{pmatrix} 1 & & \\ a & 1 & \\ & & 1 \end{pmatrix} \in GL_n(\mathbb{Z})$$

Therefore, we can simply allow P *to collect all the row reductions and* Q *to collect all of the column reductions to get the form:*

$$D = PAQ^{-1}$$

$$\iff DQ = PA$$

Since P *is an invertible matrix, we know* PA *is a matrix with the same row span as* A*. Further, we know* Q *and* DQ *will be :*

$$Q = \begin{pmatrix} \dots & y_1 & \dots \\ \dots & y_2 & \dots \\ \dots & y_3 & \dots \end{pmatrix} \quad DQ = \begin{pmatrix} \dots & a_1y_1 & \dots \\ \dots & a_2y_2 & \dots \\ \dots & \dots & \dots \end{pmatrix}$$

So DQ *will be the basis of our submodule!*
So why does simultaneous row and column reduction work?

$$\begin{pmatrix} * & * & \dots \\ * & * & \dots \\ \vdots & \vdots & \ddots \end{pmatrix} \xrightarrow{1} \begin{pmatrix} min(a_{i,j}) \neq 0 & * & \dots \\ * & * & \dots \\ \vdots & \vdots & \ddots \end{pmatrix} \xrightarrow{2} \begin{pmatrix} m \neq 0 & * & \dots \\ r_{21} & * & \dots \\ r_{31} & * & \dots \\ \vdots & \vdots & \ddots \end{pmatrix} \xrightarrow{3\dots} \dots \xrightarrow{Termination} \begin{pmatrix} d_{11} & 0 \\ 0 & A_2 \end{pmatrix}$$

1. *Identify the minimum element of absolute value within the PID and apply a permutation matrix to bring that matrix to the top-left corner.*

2. *If this new pivot divides all of the elements below it, we can zero out the other elements of this column. On the other hand, we can use the division algorithm to reduce everything within the matrix since*

$$a_{21} = mq + r_{21}$$

$$a_{31} = mq + r_{31}$$

$$\vdots$$

   so $r < m$ *or* $r = 0$.

3. *Identify a new nonzero minimum to replace the pivot in the top right-hand corner. Return to step 1.*

4. *(Termination) Once the top row pivot has zeroed out all of the adjacent column and row entries, we can then perform the same operations on the subprincipal matrix* A_2 *by excluding changes to the first row and column. We can perform this procedure inductively until we result in a diagonal matrix.*

Further, this algorithm can be used to identify the Smith Normal Form: For a matrix $A \in \mathbb{M}_n(R)$, where R is a PID, then the Smith Normal Form of A is obtained as some PAQ^{-1} with $P, Q \in GL_n(R)$ such that

$$PAQ^{-1} = \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & a_1 & & & & \\ & & & & \ddots & & & \\ & & & & & a_m & & \\ & & & & & & 0 & \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{pmatrix}$$

where $a_i | a_{i+1}$ where a_i not not units and $a_i \neq 0$. You get to do this procedure on the homework.

Recall cyclic modules are isomorphic to some quotient R/I where I is a left ideal. Since R is a PID, then we know that any cyclic module is isomorphic to $R/\langle a \rangle$ for some a.

Theorem 5.35 (Fundamental Theorem, Existence of the Invariant Form)**.** *Let R be a PID and let M be a finitely generated R-module.*

1. *Then M is isomorphic to the direct sum of finitely many cyclic modules. More precisely,*

$$M \cong R^r \oplus R/\langle a_1 \rangle \oplus R/\langle a_2 \rangle \oplus \ldots \oplus R/\langle a_m \rangle$$

   for some integer $r \geq 0$ and nonzero element $a_1, \ldots, a_m \in R$ which are not units in R and which satisfy the divisibility relations $a_1 | a_2 | \ldots | a_m$.

2. *M is torsion free if and only if M is free.*

3. *In the decomposition in (1),*

$$Tor(M) \cong R/\langle a_1 \rangle \oplus R/\langle a_2 \rangle \oplus \ldots \oplus R/\langle a_m \rangle$$

   In particular, M is a torsion module if and only if $r = 0$ and in this case the annhilator of M is the ideal $\langle a_m \rangle$.

Here, we will refer to r as the fake rank of M.

Proof. 1. Let $\langle x_1, \ldots, x_m \}$ be the generators of M and

$$\pi : R^n \to M$$
$$e_i \to x_i$$

such that $Im(\pi) = M \cong R^n / Ker(\pi)$. By a previous theorem, we know that $Ker(\pi) \subset R^n$ is a free rank $m \leq n$ module with basis $\langle a_1 y_1, \ldots, a_m y_m \}$ where $\{y_1, \ldots, y_n\}$ is another basis of R^n and $a_1 | a_2 | \ldots | a_m$. So

$$M \cong \bigoplus_{i=1}^{n} Ry_i / \bigoplus_{j=1}^{m} Ra_j y_j \cong R/\langle a_1 \rangle \oplus R/\langle a_2 \rangle \oplus \ldots \oplus R/\langle a_m \rangle \cong \underbrace{R \oplus \ldots \oplus R}_{n-m} \cong \bigoplus_{i=1}^{m} Ry_i / \left(\bigoplus_{j=1}^{m} Ra_j y_j \right) \oplus \bigoplus_{i=m+1}^{n} Ry_j$$

   Note if $\langle a_i \rangle = 1 = R$, then $R/\langle a_i \rangle = 0$. So we can ignore these and remove them from our list.

2. Now if (2) is free, we know that it is torsion free. Otherwise, if $a \neq 0$ and not a unit, then $R/\langle a \rangle$ is torsion. Since M is torsion free, this implies that no such a's exists, so $M \cong R^{n-m}$, which is free.

3. Notice $Ann(R/\langle a \rangle) = \langle a \rangle$ and since all $a_i | a_m \implies \langle a_m \rangle \subset \langle a_i \rangle$. So $\langle a_m \rangle$ annihilates $R/\langle a_i \rangle$.

■

Recall, the a_i are the invariant factors of M and $r =$ the fake rank.
Now we can see the Chinese Remainder Theorem applies to give an interesting theorem.

Theorem 5.36 (Elementary Division Form)**.** *Let R be a PID, M be a finitely generated R-module. Then*

$$M \cong R^r \oplus R/\langle p_1^{\alpha_1}\rangle \oplus R/\langle p_2^{\alpha_2} \oplus \ldots \oplus R/\langle p_t^{\alpha_t}$$

where $r \geq 0, a_i \in \mathbb{Z}_{\geq 1}, p_i \in R$ are prime.

Here, then $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ are the elementary divisors of M.

Definition 5.37. *Let $M \neq 0$ be a finitely generated module of a PID R and $\langle a\rangle = Ann(A)$. Let p be a prime dividing a. Then p-primary component of M if the submodule*

$$N = \{m \in M : p^n m = 0 \text{ for some } n >> 0\}$$

Note 5.38. *It suffices to take n so $p^n | a, p^{n+1} \not| a$.*

Remark 5.39. *It is easy to show that N is a direct summand of M. In fact,*

$$N \cong R/\langle p^{\alpha_1}\rangle \oplus R/\langle p^{\alpha_2}\rangle \oplus \ldots \oplus R/\langle p^{\alpha_k}\rangle$$

taking all the terms $p_i = p$.

Example 5.40. *Let $R = \mathbb{Z}$ and $p = 2$. Then*

$$M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$$

Lemma 5.41. *Let R be a PID and pick a prime element $p \in R$. Let $F = R/\langle p\rangle$ be a field since R is a PID. Then*

1. *If $M \cong R^r$, then $M/pM \cong F^r$ as an F-module isomorphism and as an R-module isomorphism.*
2. *Let $a \neq 0$ in R and $M = R/\langle a\rangle$. Then*

$$M/pM \cong \begin{cases} F & p|a \text{ in } R \\ 0 & \text{otherwise} \end{cases}$$

3. *If $M = R/\langle a_1\rangle \oplus \ldots \oplus R/\langle a_k\rangle$ where $p|a_i$ for all $1 \leq i \leq k$, then $M/pM \cong F^k$ as an F-module isomorphism and as an R-module isomorphism.*

Proof. Left as an exercise. ∎

Example 5.42. *Let $N = \mathbb{Z}/15\mathbb{Z}$. Since 2 is a unit, then $N/2N = 0$*

Example 5.43. *Returning to the previous example, let $R = \mathbb{Z}$ and $p = 2$. Then*

$$M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}$$

Doing each term separately,

$$\mathbb{Z}/2\mathbb{Z}/2\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$$

$$\mathbb{Z}/8\mathbb{Z}/2\mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$$

$$\mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$$

So we see that

$$M/2M = (\mathbb{Z}/2\mathbb{Z})^4$$

and $\langle 2\rangle$ is maximal everywhere.
Now, consider

$$
\begin{aligned}
&M' = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \\
&\cup \\
&2M' = 0 \oplus 2\mathbb{Z}/8\mathbb{Z} \oplus 2\mathbb{Z}/8\mathbb{Z} \\
&\cup \\
&4M' = 0 \oplus 4\mathbb{Z}/8\mathbb{Z} \oplus 4\mathbb{Z}/8\mathbb{Z} \\
&\cup \\
&8M' = 0 \oplus 0 \oplus 0
\end{aligned}
$$

Checking the factors, we see:

$$
\begin{aligned}
M'/2M' &\cong \mathbb{F}_2^3 \\
2M'/4M' &\cong \mathbb{F}_2^2 \\
4M'/8M' &\cong \mathbb{F}_2^2 \\
8M' &\cong \{0\}
\end{aligned}
$$

We can then reconstruct M' from dim 3, dim 2, dim 2, and dim 0 data. We can use this to prove the uniqueness in elementary divisor and invariant factor forms. First, if $R^{r_1} \cong R^{r_2}$, then we can go to $R^{r_i}/pR^{r_i} \cong F^{r_i}$ to see that $r_1 = r_2$ since vector space dimension is invariant!
If M has 2 expressions M_1, M_2, then

$$
Tor(M_1) \cong Tor(M_2) \implies \underbrace{M_1/Tor(M_1)}_{\cong R^{r_1}} \cong \underbrace{M_2/Tor(M_2)}_{\cong R^{r_2}}
$$

Therefore, it must be true that $r_1 = r_2$.
Now, looking at the Torsion component, got to $Tor(M_1) \cong Tor(M_2)$. Where

$$
Tor(M_1) = \bigoplus_{\langle p \rangle \supset Ann(Tor(M_1))} p - Primary\ Components
$$

Picking a prime p with $\langle p \rangle \supset Ann(Tor(M_i))$ and compare p-primary components N_1, N_2. Either by induction or reconstructively what elementary divisors must be. So $N_1 \cong N_2, pN_1 \cong pN_2, p^2N_1 \cong p^2N_2, \ldots$. So

$$
p^k N_1/p^{k+1}N_1 \cong p^k N_2/p^{k+1}N_2 \cong \mathbb{F}^{d_k}
$$

where $\mathbb{F} = R/\langle p \rangle$.

$$
N_1 \cong R/\langle p^{e_1} \rangle \oplus R/\langle p^{e_2} \rangle \ldots
$$

to reconstruct e_i. So Unique elementary divisors implies unique invariant factors.

5.3 Rational Canonical Form

Let $R = \mathbb{F}[x]$. Then we can port a lot of our familiar linear algebra concepts to this realm.
If $A \in M_n(\mathbb{F})$, then A is equivalent to an $\mathbb{F}[x]$-module V with $dim_{\mathbb{F}}(V) = n$. Therefore, we can in fact leverage module theory in order to prove some of the familiar concepts we have from linear algebra.
Since $dim_{\mathbb{F}}\mathbb{F}[x] = \infty$, we know that V is finitely generated then V must be torsion. Otherwise, it will have a free component of infinite dimension, which contradicts the finite generation. So by the fundamental theorem , we can represent

$$
V \cong \bigoplus_{i=1}^{k} \mathbb{F}[x]/\langle a_i \rangle
$$

with $a_1|a_2|\dots|a_k$. We can also represent it as:

$$V \cong \bigoplus_{i=1}^{r} \mathbb{F}[x]/\langle p_i^{e_i}\rangle$$

The invariant invariant factor form yields the Rational Canonical Form of a matrix A, by taking a basis $\{1, x, x^2, \dots\}$ for $\mathbb{F}[x]/\langle a\rangle$.
On the other hand, the Elementary Divisor Form, with basis $\{p^{e-1}, p^{e-2}, \dots, p, 1\}$ for $\mathbb{F}[x]/\langle p^e\rangle$ yields that Jordan Normal Form.
Recall, if A is a $n \times n$ matrix, its characteristic polynomial is

$$char_A(x) = det(xI_n - A)$$

Recall $char_A(x)$ is a degree n polynomial whose roots are the eigenvalues of A.
If $A \in \mathbb{M}_n(\mathbb{F})$, roots of the $char_A(x)$ might not live in $\mathbb{F}$ but in some field extension.

Definition 5.44. *The minimal polynomial of A $min_A(x)$ is the monic polynomial such that*

$$\langle min_A(x)\rangle = Ann(\text{the } \mathbb{F}[x]\text{-module } V \text{ determined by } A)$$

Theorem 5.45 (Cayley-Hamilton)**.** *$char_A(A) = 0$ in $\mathbb{M}_n(\mathbb{F})$.*

Corollary 5.45.1. *$min_A(x)|char_A(x)$ in $\mathbb{F}[x]$.*

Remark 5.46. *An alternate approach: look at $I_n, A, A^2, A^3, \dots$ until we find a dependence relation in $\mathbb{F}$-vector space $\mathbb{M}_n(\mathbb{F})$.*

Note 5.47. *$min_A(x)$ and $char_A(x)$ have the same roots in $\overline{\mathbb{F}}$ but the multiplicities in min can be smaller, but still greater than or equal to 1.*

Example 5.48. *Consider*

$$A = \begin{pmatrix} 2 & 1 & & & & & & \\ & 2 & 1 & & & & & \\ & & 2 & & & & & \\ & & & 2 & 1 & & & \\ & & & & 2 & & & \\ & & & & & 3 & & \\ & & & & & & 3 & \end{pmatrix}$$

Then $char_A(x) = det(xI_7 - A) = (x-2)^5(x-3)$ and $min_A(x) = (x-2)^3(x-3)$.

Note 5.49. *Any zero main diagonal $n \times n$ matrix J satisfies $J^n = 0$. These are usually called nilpotent matrices in linear algebra.*

Example 5.50. $J = \underbrace{\begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & 1 & \\ & & & \ddots & \ddots \\ & & & & 0 \quad 1 \end{pmatrix}}_{n \times n}$ *satisfies $J^n = 0$ but $J^{n-1} \neq 0$.*

Example 5.51. *We can also identify a $\mathbb{Z}$-analogy. Specifically, we can consider a $\mathbb{Z}$-module*

$$M = \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

Example 5.52. *The difference between the characteristic polynomial and the minimal polynomial can be illustrated by considering the $\mathbb{Z}$-analogy of this decomposition:*

$$M = \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$$

Notice, $|M| = 2^5 \cdot 3^2$ and $Ann(M) = 8 \cdot 3 = 2^3 \cdot 3^1$.

Example 5.53. *Consider the case where all of the elementary factors are powers of 3. Clearly,*

$$Ann(\mathbb{Z}/3^n\mathbb{Z}) = \langle 3^n \rangle$$

Moreover, we see that

$$Ann(\mathbb{Z}/3^{n_1}\mathbb{Z} \oplus \mathbb{Z}/3^{n_2}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/3^{n_k}\mathbb{Z}) = \langle 3^{\max\{n_i\}} \rangle = lcm\{3^{n_i}\}_{i=1}^{k} = \bigcap_{i=1}^{k} \langle 3^{n_i} \rangle$$

In particular,

$$Ann([\mathbb{Z}/3^2\mathbb{Z} \oplus \mathbb{Z}/3^4\mathbb{Z} \oplus \mathbb{Z}/3^4\mathbb{Z}] \oplus [\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5^3\mathbb{Z}]) = \langle 3^4 \cdot 5^3 \rangle$$

Example 5.54. *This idea of using the lcm is similar to understanding the minimality of the Jordan Blocks:*

$$\min \begin{pmatrix} J_2(3) & 0 & 0 & 0 & 0 & 0 \\ 0 & J_4(3) & 0 & 0 & 0 & 0 \\ 0 & 0 & J_4(3) & 0 & 0 & 0 \\ 0 & 0 & 0 & J_1(5) & 0 & 0 \\ 0 & 0 & 0 & 0 & J_1(5) & 0 \\ 0 & 0 & 0 & 0 & 0 & J_3(5) \end{pmatrix} = (x-3)^4(x-5)^3$$

Further, if $J_n(0) = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & \ddots & \\ & & & \ddots & 1 \\ & & & & 0 \end{pmatrix}$, then $min_{J_n(0)}(x) = x^n$. Moreover,

$$min \begin{pmatrix} J_{n_1}(0) & & & & \\ & J_{n_2}(0) & & & \\ & & J_{n_3}(0) & & \\ & & & \ddots & \\ & & & & J_{n_k}(0) \end{pmatrix} = lcm(\min_{J_{n_i}}(0)(x)) = x^{\max\{n_i\}}$$

So we see that

$$J_n(\lambda) = \lambda I_n + J_n(0) = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \lambda & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix}$$

And since we are simply translating, it must follow that

$$min_{\lambda I_n + J_n(0)} = (x-\lambda)^n$$

So it should be easy to see that there is a correspondence between $J_n(\lambda)$ and the $\mathbb{F}[x]$-module $\mathbb{F}[x]/\langle (x-\lambda)^n \rangle$. In a similar way, for a finitely generated $\mathbb{F}[x]$-module V, then we know that

$$V \cong \oplus \text{ of the invariant factors of } A$$

So $char_A(x) = \prod$invariant factors $= \prod$elementary divisors. On the other hand, $min_A(x) = a_m$ is the least invariant factor, since $a_i | a_m$ and any prime factor of a_i is also a prime factor of a_m.

Remark 5.55. *Elementary divisors can change if we enlarge $\mathbb{F} \subset K$ since formerly formerly irreducible polynomials can factor. But invariant factors do not change!*

Corollary 5.55.1. *Let A and B be two $n \times n$ matrices over a field F and suppose $\mathbb{F}$ is a subfield of the field K.*

1. *The rational canonical form of A is the same whether it is computed over K or over F. The minimal and characteristic polynomials and the invariant factors of A are the same whether A is considered as a matrix over F or a matrix over K.*

2. *The matrices A and B are similar over K if and only if they are similar over F.*

Example 5.56. *Consider $V_{\mathbb{R}} = \mathbb{R}[x]/\langle x^2+1\rangle$ and $V_{\mathbb{C}} = \mathbb{C}[x]/\langle x^2+1\rangle$. As an $\mathbb{R}[x]$, it's already in invariant factor and elementary divisor form. On the other hand, it is only in invariant factor form over $\mathbb{C}$ and the elementary divisor form is:*

$$\mathbb{C}[x]/\langle x-i\rangle \oplus \mathbb{C}[x]/\langle x+i\rangle$$

Definition 5.57. *Given a monic polynomial $a(x) = x^k + \ldots + b_2x^2 + b_1x + b_0 \in \mathbb{F}[x]$ be monic. Then the companion matrix is the $k \times k$ matrix of a_0, written*

$$C_{a(x)} = \begin{pmatrix} 0 & & & & & -b_0 \\ 1 & 0 & & & & -b_1 \\ & 1 & 0 & & & -b_2 \\ & & 1 & \ddots & & \vdots \\ & & & \ddots & 0 & -b_{k-2} \\ & & & & 1 & -b_{k-1} \end{pmatrix}$$

You should recognize this as the matrix of multiplication of x on the module $V = \mathbb{F}[x]/\langle a(x)\rangle$ with respect to the basis $\{1, x, x^2, \ldots, x^{k-1}\}$.

Definition 5.58. *A matrix is in the rational canonical form if it is block diagonal with form:*

$$\begin{pmatrix} C_{a_1(x)} & & & & \\ & C_{a_2(x)} & & & \\ & & C_{a_3(x)} & & \\ & & & \ddots & \\ & & & & C_{a_m(x)} \end{pmatrix}$$

where $a_i | a_{i+1}$ in $\mathbb{F}[x]$ and $a_i(x)$ are monic. Here, the $a_i(x)$ are also called the invariant factors of the matrix.

Remark 5.59. *If $\sum_{i=1}^m deg(a_i(x)) = n$ and $V = \mathbb{F}^n$ with the $\mathbb{F}[x]$-module structure given by x acts on*

$$\begin{pmatrix} C_{a_1(x)} & & & & \\ & C_{a_2(x)} & & & \\ & & C_{a_3(x)} & & \\ & & & \ddots & \\ & & & & C_{a_m(x)} \end{pmatrix}$$

then $V \cong \mathbb{F}[x]/\langle a_1(x)\rangle \oplus \ldots \mathbb{F}[x]/\langle a_m(x)\rangle$ and V is a finitely generated torsion $\mathbb{F}[x]$-module with invariant factors $a_1, \ldots, a_m$.

So the decomposition theorem shows that any matrix $A \in \mathbb{M}_n(\mathbb{F})$ is similar to a matrix in Rational Canonical Form. And this form is in fact unique.

Question 5.60. *Given a matrix A, how do we find the Rational Canonical Form?*

1. You can go to the elementary divisor form and then come back. This is a bit ad hoc.

2. The more traditional way of computing the Rational Canonical Form is done by a similar process of finding the eigenvalues of A. So consider $xI_n - A \in \mathbb{M}_n(\mathbb{F}[x])$ and put it into Smith Normal Form by row reducing over the PID $\mathbb{F}[x]$. So we end up with

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & a_1(x) & & \\ & & & & \ddots & \\ & & & & & C_{a_m(x)} \end{pmatrix}$$

such that $a_i(x)|a_{i+1}(x)$ are monic polynomials.

How do we set this up? Returning to the $\mathbb{Z}$-analogy, we understand that for a finitely generated torsion $\mathbb{Z}$-module N, we can realize it via a mapping $\mathbb{Z}^n \to N$ by

$$\mathbb{Z}^n \xrightarrow{\phi} \underbrace{\mathbb{Z}^n}_{\supset M} \xrightarrow{\pi} N$$

Then we can apply our submodule of a free module over a PID theorem to align some basis $\{y_1, \ldots, y_n\}$ over $\mathbb{Z}^n$ so that we have a basis $\{a_1 y_1, \ldots, a_m\}$ over M. Then by identifying the Smith Normal Form, we can a matrix for ϕ, say B and then have PBQ^{-1} to find $a_1|a_2|\ldots|a_m$. So

$$N \cong \mathbb{Z}^n/M \cong \mathbb{Z}/\langle a_1\rangle \oplus \ldots \mathbb{Z}/\langle a_m\rangle$$

Doing this for $R = \mathbb{F}[x]$, we want

$$\mathbb{F}[x]^n \xrightarrow{\phi} \underbrace{\mathbb{F}[x]^n}_{\supset M} \xrightarrow{\pi} V$$

But now $\phi(x) := xI_n - A$.

Example 5.61. *Given $V = \mathbb{F}[x]/\langle x-2\rangle \leftrightarrow$ a 1 dimensional $\mathbb{F}$ vector space with $A = 2$. So this means that x acts as 2, so $xI_1 - A = x[1] - [2] = [x-2]$.*

Example 5.62. *Let $W = \mathbb{F}^2$ where $A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$. So x acts as 2 on $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and x acts as 2 on $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. So*

$$\mathbb{F}[x]/\langle x-2\rangle \oplus \mathbb{F}[x]/\langle x-2\rangle \cong \mathbb{F}[x] \oplus \mathbb{F}[x]/\langle x-2\rangle\mathbb{F}[x] \oplus \langle x-2\rangle\mathbb{F}[x] \cong \mathbb{F}[x] \oplus \mathbb{F}[x]/\left\langle \begin{pmatrix} x \\ 0 \end{pmatrix} - \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x \end{pmatrix} - \begin{pmatrix} 0 \\ 2 \end{pmatrix} \right\rangle$$

$$\cong \mathbb{F}[x] \oplus \mathbb{F}[x]/\langle \textit{Image of } \phi\rangle$$

where $\phi = x \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = xI_2 - A$.

So saying that x acts as A on $\mathbb{F}^n$ is the same as saying that $Im(xI_n - A)$ acts as 0 on $\mathbb{F}[x]^n$. So we can put $xI_n - A$ into Smith Normal Form in order to recover a_i to yield

$$\mathbb{F}[x]^n/Im(\phi) \cong \mathbb{F}[x]/\langle a_1\rangle \oplus \ldots \oplus \mathbb{F}[x]/\langle a_m\rangle$$

with $a_i|a_{i+1}$.

5.4 Jordan Normal Form

Assume $char_A(x)$ splits over $\mathbb{F}$. So A and $n \times n$ matrix corresponds with an $\mathbb{F}[x]$-module of the form

$$\mathbb{F}[x]/\langle (x-\lambda_1)_1^e \rangle \oplus \mathbb{F}[x]/\langle (x-\lambda_k)_k^e \rangle$$

where the characteristic polynomial $char_A(x) = \prod_{i=1}^{l}(x-\lambda_i)^{e_i}$ and $e_i \geq 1$. Note, the λ_i not not be distinct. Then A is similar to

$$\begin{pmatrix} J_{e_1}(\lambda_1) & & & & \\ & J_{e_2}(\lambda_2) & & & \\ & & J_{e_3}(\lambda_3) & & \\ & & & \ddots & \\ & & & & J_{e_k}(\lambda_k) \end{pmatrix}$$

There is no special ordering of the blocks, we could order by λ's if $\mathbb{F}$ is order, or by the magnitude of e_i, but there is no assumption on the resultant order. Now,

$$min_A(x) := lcm\{(x-\lambda_i)^{e_i}\}_i$$

To find the lcm, we look at each λ to find NullSpace$((\lambda I - A)^m)$ where $(x-\lambda)^m | char_A(x), (x-\lambda)^{m+1} \nmid char_A(x)$. Then we see that

$$NS((\lambda I - A)^{m-1}) \supset NS((\lambda I - A)^{m-2}) \supset \ldots \supset NS(\lambda I - A)$$

Much like our homework problem

$$M \supset 2M \supset 4M \supset 8M \supset 16M \supset \ldots$$

Then we see that $M/2M, 2M/4M, \ldots$ and their $\mathbb{F}_2$ dimension, and we notice the jumps and stutters in order to recover $\mathbb{Z}/2^k\mathbb{Z}$ in M. So we can do the same here to find $J_{k_i}(\lambda)$

Example 5.63.

$$A = \begin{pmatrix} J_4(0) & & & & & & \\ & J_4(0) & & & & & \\ & & J_2(0) & & & & \\ & & & J_2(0) & & & \\ & & & & J_2(0) & & \\ & & & & & J_1(0) \end{pmatrix}$$

then $char_A(x) = x^15$ *while* $min_A(x) = x^4$. *Seeing the dimension of the null spaces, we get :*

$$dim(NS(A^15))) = dim(A^4) = 15$$

$$dim(NS(A^3))) = 15 - 2 = 13$$

$$dim(NS(A^2))) = 15 - 4 = 11$$

$$dim(NS(A))) = 15 - 9 = 6$$

Notice, this related to

$$dim(J_4(0)) = 1$$

$$dim(J_4(0)^2) = 2$$

$$dim(J_4(0)^3) = 3$$

$$dim(J_4(0)^4) = 4$$

Remark 5.64. *Suppose we wanted to find the actual basis that makes a matrix in Jordan Form. It's a huge pain to actually do this.*

Example 5.65.

$$A = \begin{pmatrix} 0 & 1 & & & & \\ & 0 & 1 & & & \\ & & 0 & 1 & & \\ & & & 0 & & \\ & & & & 0 & 1 \\ & & & & & 0 \end{pmatrix}$$

is already in Jordan Block Form. We see that:

$$NS(A) = span \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Then

$$A^2 = \begin{pmatrix} 0 & 0 & 1 & & & \\ & 0 & 0 & 1 & & \\ & & 0 & 0 & & \\ & & & 0 & & \\ & & & & 0 & 0 \\ & & & & & 0 \end{pmatrix} \implies NS(A^2) = span \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

And

$$A^3 = \begin{pmatrix} 0 & 0 & 0 & 1 & & \\ & 0 & 0 & 0 & & \\ & & 0 & 0 & & \\ & & & 0 & & \\ & & & & 0 & 0 \\ & & & & & 0 \end{pmatrix} \implies NS(A^2) = span \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$A^4 = \begin{pmatrix} 0 & 0 & 0 & 0 & & \\ & 0 & 0 & 0 & & \\ & & 0 & 0 & & \\ & & & 0 & & \\ & & & & 0 & 0 \\ & & & & & 0 \end{pmatrix} \implies NS(A^2) = span \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$