ALGEBRA III NOTES

NICHOLAS HAYEK

Lectures by Prof. Henri Darmon

CONTENTS

I   Groups

8/28/24

In Algebra 3, we will study abstract algebraic structures. Chiefly among them, we have *groups*, which are useful in representing symmetries, *rings & fields*, which help us think about number systems, and *vector spaces & modules*, which encode physical space.

<div align="center">AXIOMS AND FIRST PROPERTIES</div>

A *group* is a set G endowed with a binary composition $G \times G \to G$ such that the following axioms hold:

DEF 1.1

1. $\exists e \in G$, an identity element, such that $e * a = a * e = a \ \forall a \in G$.

2. $\forall a \in G, \exists a' \in G$ such that $a * a' = a' * a = e$.

3. $a * (b * c) = (a * b) * c \ \forall a, b, c \in G$.

If $a * b = b * a \ \forall a, b \in G$, we call G *commutative*.

DEF 1.2

Why do we care about groups? If X is an object, we call a *symmetry* of X a function $X \to X$ which preserves the structure of the object.

e.g. a polygon, graphs, tilings, "crystal," "molecules," rings, vector spaces, metric spaces, manifolds

The collection of symmetries, $\mathrm{Aut}(X) = \{f : X \to X\}$, we can structure as a group: let $* = \circ$, $e = \mathrm{Id}$, and $f \in \mathrm{Aut}(X)$ (note that, by axiom 2, these must be bijective).

A note on notation: for non-commutative groups, we write $a * b = ab$, $e = 1$ or $\mathbb{1}$, $a' = a^{-1}$, and $a^n = \underbrace{a \cdot ... \cdot a}_{n \text{ times}}$. This is called *multiplicative notation*. For commutative rings, we write $a * b = a + b$, $e = 0$ or $\mathbb{0}$, $a' = -a$, and $na = \underbrace{a + ... + a}_{n \text{ times}}$.

<div align="center">♠ Examples ♣</div>

E.G. 1.1

1. If X is a set with no operations, $\mathrm{Aut}(X)$ is the set of all bijections $f : X \to X$. One calls this the *permutation group*, or, if $|X| = n < \infty$, the *symmetric group*, and we write $\mathrm{Aut}(X) = S_n$.

2. If V is a vector space over $\mathbb{F}$, $\mathrm{Aut}(V) = \{T : V \to V\}$, the set of vector space isomorphism. If $\dim(V) = n$, recall that we associate V with $\mathbb{F}^n$, whose set of isomorphism is given by $GL_n(\mathbb{F})$, the collection of $n \times n$ invertible matrices. This is called the *linear group*.

3. If R is a ring, then $(R, +, \mathbb{0})$ is a commutative group. Furthermore, $(R^\times, \times, \mathbb{1})$ is a non-commutative group, where $R^\times := R \setminus \{\text{non-invertible elements of } R\}$.

4. If V is Euclidean space endowed with a dot product, where $\mathbb{F} = \mathbb{R}$, with $\dim(V) < \infty$, $\mathrm{Aut}(V) = O(V)$ is called the *orthogonal group of* V. In particular, $O(V) = \{T : V \to V : T(u) \cdot T(v) = u \cdot v\}$.

5. If X is a geometric figure (e.g. a polygon), we write $\mathrm{Aut}(X) = D_n$, where $|\mathrm{Aut}(X)| = n$, and call this the *dihedral group*.

DEF 1.3

A *homomorphism* from groups $G_1 \to G_2$ is a function $\varphi : G_1 \to G_2$ satisfying $\varphi(ab) = \varphi(a)\varphi(b)$, where $a, b \in G_1$.

PROP 1.1

$\varphi(\mathbb{1}_{G_1}) = \mathbb{1}_{G_2}$ and $\varphi(a^{-1}) = \varphi(a)^{-1}\ \forall a \in G_1$.

PROOF.

$$\varphi(\mathbb{1}_{G_1}) = \varphi(\mathbb{1}_{G_1}^2) = \varphi(\mathbb{1}_{G_1})^2 \implies \varphi(\mathbb{1}_{G_1}) = \varphi(\mathbb{1}_{G_1}^{-1})\varphi(\mathbb{1}_{G_1}) = \mathbb{1}_{G_2}.$$

$$\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(\mathbb{1}_{G_1}) = \mathbb{1}_{G_2} \implies \varphi(a_{-1}) = \varphi(a)^{-1}. \qquad \square$$

DEF 1.4

A homomorphism which is bijective is called an *isomorphism*. If there exists an isomorphism between two groups G_1 and G_2, we call them *isomorphic*, and write $G_1 \cong G_2$. One can thus call $\mathrm{Aut}(G)$ the set of isomorphisms from $G \to G$.

As an example, take $G = \mathbb{Z}/n\mathbb{Z} = \{0, 1, ..., n-1\}$. Note that $\varphi : G \to G$ is determined entirely by $\varphi(1)$, since $\varphi(i) = \varphi(\underbrace{1 + ... + 1}_{i \text{ times}}) = \underbrace{\varphi(1) + ... + \varphi(1)}_{i \text{ times}}$. How can we find an element of $\mathrm{Aut}(G)$? Clearly, not all mappings $\varphi(1)$ are bijective: take n to be even and $\varphi(1) = 2$. Then $\varphi(2) = 4$, $\varphi(3) = 6$, ..., $\varphi(n/2) = 0$, so φ is not surjective. We know then that $\varphi(G) = \varphi(1)\mathbb{Z} \mod n$, and would like $\varphi(G) = G$. If $\varphi(1)$ and n are co-prime, then we can write $k\varphi(1) + ln = k\varphi = 1$, so every element can be reached.

We can construct a group isomorphism $\eta : \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ which sends $\varphi \to \varphi(1)$. Clearly $\eta(\varphi_{t_1} \circ \varphi_{t_2}) = \varphi_{t_1} \circ \varphi_{t_2}(1) = \varphi_{t_1}(t_2) = t_1 t_2 = \eta(\varphi_{t_1})\eta(\varphi_{t_2})$, so η is a homomorphism. It is also bijective: given $\varphi(1)$, we can deduce a mapping for each element.

DEF 1.5

For a group G and an object X, define an *action* to be a function from $G \times X \to X$ such that

1. $\mathbb{1} \times x = x$

2. $(g_1 g_2)x = g_1(g_2 x)$

for $x \in X$, $g_1, g_2 \in G$. One can create from this the automorphism $m_g : x \to gx$ of X: if $gx_1 = gx_2$, one can take the group inverse to conclude $x_1 = x_2$. Similarly, given $x \in X$, we know $m_g(g^{-1}x) = x$.

Given an action of G on X, the assignment $g \rightarrow m_g$ is a homomorphism between $G \rightarrow \text{Aut}(X)$.

$$m_{g_1 g_2}(x) = g_1 g_2 x = g_1(g_2 x) = g_1 m_{g_2}(x) = m_{g_1}(m_{g_2}(x)) = m_{g_1} \circ m_{g_2}(x) \qquad \square$$

In fact, given a homomorphism of this form, one can extract the group action.

A *G-set* is a set X endowed with a group action of G. If $\forall x, y \in X, \exists g \in G : gx = y$, we say that this G-set is *transitive*. Finally, a transitive G-set of a subset of X ("G-subset of X") is called an *orbit* of G on X.

Every G-set is a disjoint union of orbits.

We define a relation on X as follows: $x \underset{G}{\sim} y$ if $\exists g : gx = y$. This is an equivelance relation:

1. Take $g = \mathbb{1}$. Then $\mathbb{1}x = x$, so $x \underset{G}{\sim} x$.

2. If $gx = y$, then $g^{-1}y = x$, so $x \underset{G}{\sim} y \implies y \underset{G}{\sim} x$.

3. If $gx = y$ and $hy = z$, then $hgx = z$, so $x \underset{G}{\sim} y \land y \underset{G}{\sim} z \implies x \underset{G}{\sim} z$.

From prior theory, we know that equivalence classes of an equivalence relation on X form a partition of X. However, by definition, the equivalence classes of the above relation are exactly the orbits of the G-set on X. $\qquad \square$

We denote the set of equivalence classes defined in the proof above X/G.

───────────────── ♠ *Examples* ♣ ─────────────────

1. Let $X = \{\clubsuit\}$, G be a group, and $g\clubsuit = \clubsuit$. This is a group action. The homomorphism $m : G \rightarrow \text{Aut}(X) = S_1$ sends g to the identity.

2. Let $X = G$, G be a group, and $gx = gx$ (group action on the LHS, left-multiplication on the RHS). We have the homomorphism $m : G \rightarrow \text{Aut}(G)$ such that $m(g)(x) = gx = gx$. This is an injective function, since we can always take the group inverse, i.e. $m(h)(x) = m(g)(x) \implies g = h$. Thus, $G \cong m(G) \subseteq \text{Aut}(G)$.

3. Let $X = G$ as before, but let $gx = xg^{-1}$. We can check that this is a group action: (1) $\mathbb{1} * x = x\mathbb{1}^{-1} = x\mathbb{1} = x$ and (2) $g * (h * x) = (h * x)g^{-1} = xh^{-1}g^{-1}$, where $(gh) * x = x(gh)^{-1} = xh^{-1}g^{-1} \implies g * (h * x) = (gh) * x$.

4. Letting $X = G \times G$, we can form a group action from both left- and right-multiplication: $(g, h) * x = gxh^{-1}$. One can check its validity.

DEF 1.7 If X_1 and X_2 are G-sets, then an *isomorphism* from X_1 to X_2 is a bijection $\varphi : X_1 \to X_2$ such that $\varphi(gx) = g\varphi(x) \ \forall x \in X_1, g \in G$.

DEF 1.8 Let $H < G$. Define G/H to be the set of orbits for right action on G, i.e $\{aH : a \in G\}$, where $aH = \{ah : h \in H\}$. We call these *left cosets*. We also have *right cosets*, $\{Ha : a \in G\}$.

For example, take $G = S_3$ and $H = \{\mathbb{1}, (12)\}$. Then $G/H = \{\{\mathbb{1}, (12)\}, \{(13), (123)\}\} = \{H, (13)H\}$ and $H \setminus G = \{\{\mathbb{1}, (12)\}, \{(13), (132)\}, \{(23), (123)\}\}$.

> **1.1 Size of Cosets**
>
> Let $H < G$. If H is finite, then $|H| = |aH| \ \forall a \in G$.

As proof of this fact, one may take the bijection $\varphi : H \to aH : \varphi(h) = ah$.

> **1.2 Lagrange**
>
> Let G be finite. The cardinality of any subgroup $H < G$ divides the cardinality of G. In particular, $|G| = |H| \cdot |G/H|$.

DEF 1.9 Define the *stabilizer* of an element of a G-set $x_0 \in X$ to be $\{g \in G : g \circledast x_0 = x_0\}$.

PROP 1.4 If X is a transitive G-set, then $\exists H < G$ such that $X \cong G/H$ as a G-set.

PROOF. Choose $x_0 \in X$. Define $H = \mathrm{stab}(x_0) := \{g \in G : g \circledast x_0 = x_0\}$. One may show that H is indeed a subgroup. We then define $\varphi : G/H \to X$ such that $gH \to gx_0$. Checking some properties:

1. φ is well defined. If $gH = g'H$, then $\exists h : gh = g'$. Then $\varphi(gH) = gx_0$ and $\varphi(g'H) = g'x_0 = ghx_0$. But $h \in \mathrm{stab}(x_0)$, so this is just gx_0.

2. φ is surjective. This follows from the fact that X is transitive: for $x, x_0 \in X, \exists g \in G$ with $gx_0 = x$. Then $\varphi(gH) = gx_0 = x$.

3. φ is injective. Take $g_1 x_0 = g_2 x_0$. Then $g_2^{-1} g_1 x_0 = x_0$, so $g_2^{-1} g_1 \in H$, i.e. $g_2 H = g_1 H$

4. φ is a G-set isomorphism. $\varphi(g \circledast aH) = \varphi(gaH) = gax_0 = g\varphi(aH)$. $\quad \square$

> **1.3 Orbit-Stabilizer**
>
> If X is a transitive G-set, $x_0 \in X$, and $|G| < \infty$, then $X \cong G/\mathrm{stab}_G(x_0)$. In particular, $|G| = |X| \cdot |\mathrm{stab}_G(x_0)|$

Given $H < G$, we say $h_1, h_2 \in H$ are *conjugate* if $\exists g : g^{-1} h_1 g = h_2$, or, equivalently, $\quad$ DEF 1.10
$gh_1 g^{-1} = h_2$. Given $H_1, H_2 < G$, we say H_1 and H_2 are *conjugate equivalent* if every
element in H_1 is conjugate to some element in H_2.

Stabilizers of elements in a transitive G-set X are conjugate equivalent. $\quad$ PROP 1.5

> Let $x_1, x_2 \in X$ and consider stab(x_1), stab(x_2). Since X is transitive, $\exists g : gx_1 =$ $\quad$ PROOF.
> x_2. Thus, if $h \in$ stab(x_2), i.e. $hx_2 = x_2$, then $hgx_1 = gx_1 \implies g^{-1}hgx_1 =$
> $x_1 \implies g^{-1}hg \in$ stab(x_1). Thus, there exists a conjugation of every element
> in stab(x_2) which is an element in stab(x_1). One shows the converse similarly
> to conclude that stab(x_1) and stab(x_2) are conjugate equivalent. $\qquad \square$

We can show a natural bijection between the "pointed G-sets" (X, x_0) with sub- $\quad$ PROP 1.6
groups of G: send $(X, x_0) \to$ stab(x_0) and $H \to (G/H, H)$. This establishes the
intuition that the number of transitive G-sets up to isomorphism is exactly the
number of subgroups of G up to conjugation.

> Consider an isomorphism class P of pointed G-sets, i.e. $\forall (X, x_0), (Y, y_0) \in P,$ $\quad$ PROOF.
> $X \cong Y$. Consider the mapping $\Phi : (X, x_0) \in P \to$ stab(x_0). The image of
> this mapping is a conjugation class: since $X \cong Y$, we know that there exists
> a unique mapping $\varphi(y_0) = x_k$. Since X is transitive, $\exists g : gx_k = x_0$. Then
> $h \in$ stab$(x_0) \implies hx_0 = x_0 \implies hgx_k = gx_k \implies hg\varphi(y_0) = g\varphi(y_0) \implies$
> $\varphi(hgy_0) = \varphi(gy_0) \implies hgy_0 = gy_0 \implies g^{-1}hg \in$ stab(y_0).
>
> [8pt]Conversely, one can show that the image of the mapping $\Xi : H \to$
> $(G/H, H)$ over a conjugation class $I : \forall F, H \in I, \exists g \in G : g^{-1}Fg = H$ is an
> isomorphism class over G-sets.
>
> [8pt]Thus, the set of G-sets up to isomorphism is in bijection with the set of
> $H < G$ up to conjugation. $\qquad \square$

--------------------------------- ♠ *Examples* ♣ --------------------------------- $\quad$ E.G. 1.3

1. Let $H = G$. Then $G/H = \{H\}$. $X = \{*\} \cong G/H$. Similarly, if $H = \mathbb{1}$, then
   $G/H \cong G = X$.

2. Let $G = S_n$. Let $X = \{1, 2, ..., n\}$. For $n \in X$, $X \cong G/$stab$(n) = G/S_{n-1}$.

3. Let X be a regular tetrahedron. Let $G =$ Aut(X) (the set of rigid motions).
   Notate $X = \{1, 2, 3, 4\}$ (for each vertex). Then G acts transitively on X. In
   particular, stab$(1) = \mathbb{Z}3 \implies |G| = 4 \cdot 3 = 12$.

4. Let $G =$ Aut(X) on a tetrahedron, this time *including* reflections. Then
   $G = S_4$, since one can always send $a \to b$ by reflecting through a plane
   intersecting c, d.

5. Let X be a cube, $G = \text{Aut}(X)$, the rigid motions on X. Note that there are 6 faces, 12 edges, and 8 vertices. If x_0 is a face, then $\text{stab}(x_0)$ are exactly the rotations about the axis intersecting the face, i.e. $|\text{stab}(x_0)| = 4$, so $|G| = 6 \cdot 4 = 24$. As $4! = 24$, it is tempting to consider that $G \cong S_4$. This turns out to be true: let G act on the cube's diagonals.

PROP 1.7

If $\varphi : G \to H$ is a homomorphism, then φ is injective $\iff \varphi(g) = \mathbb{1} \implies g = \mathbb{1} \, \forall g \in G$.

PROOF.

> Let $\varphi(g) = \mathbb{1}$ and φ be injective. Then $\varphi(g^2) = \varphi(g) \implies g^2 = g \implies g = \mathbb{1}$.
>
> [8pt]Let $\varphi(g) = \mathbb{1} \implies g = \mathbb{1}$. Then $\varphi(a) = \varphi(b) \implies \varphi(b^{-1}a) = \mathbb{1} \implies b^{-1}a = \mathbb{1} \implies a = b$, so φ is injective. $\qquad\square$

Define $\ker(\varphi) := \{g \in G : \varphi(g) = \mathbb{1}\}$. This is a subgroup.

DEF 1.11

Observe that, for $g \in G, h \in \ker(\varphi)$, we have $g^{-1}hg \in \ker(\varphi)$. Subgroups which obey this property are called *normal subgroups*.

PROP 1.8

If N is normal, then $G/N = N/G$, i.e. $gN = Ng \, \forall g$. One can view G/N as a group with $g_1 N \cdot g_2 N = g_1 g_2 N$, and $\mathbb{1}_{G/N} = N$.

PROOF.

> $gN = \{gn : n \in N\} = \{gg^{-1}ng : n \in N\} = \{ng : n \in N\} = Ng$. The group operations follow immediately. $\qquad\square$

1.4   Isomorphism Theorem for Groups

If $\varphi : G \to H$ is a homomorphism, $N = \ker(\varphi)$, then φ induces an injective homomorphism $\overline{\varphi} : G/N \hookrightarrow H : \overline{\varphi}(aN) = \varphi(a)$.

PROOF.

> $\overline{\varphi}$ being a homomorphism follows from the fact that φ is a homomorphism. For injectivity, see that $\overline{\varphi}(aN) = \mathbb{1} \implies \varphi(a) = \mathbb{1} \implies a = \mathbb{1}$. $\qquad\square$

E.G. 1.4

———————————————————— ♠ *Examples* ♣ ————————————————————
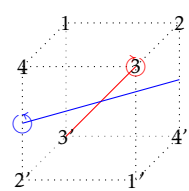
Let X be a cube, and $G = \text{Aut}(X)$ be the set of rigid motions. Consider the homomorphism $\varphi : G \to S_4$ (permutations of the diagonals). Then $\ker(\varphi) = \{\sigma \in \text{Aut}(X) : \sigma(\{ii'\}) = \{ii'\}\} = \cap_{j=1}^{4}\text{stab}(\{jj'\})$. Observe that $\text{stab}(\{ii'\})$ are exactly the 3 rotations about the axis ii' (red), the 2 perpendicular rotations (blue), as well as the identity. Observe that these rotations are disjoint, so $\cap_{j=1}^{4}\text{stab}(\{jj'\}) = \{\mathbb{1}\} \implies \ker(\varphi) = \mathbb{1}$.

Then, we have $\overline{\varphi} : G/\ker(\varphi) \hookrightarrow S_4 = G/\{\mathbb{1}\} \hookrightarrow S_4 = G \hookrightarrow S_4$ is injective. Since $|G| = |S_4|$, we have that $G \cong S_4$.

Consider now $\widetilde{G} = \widetilde{\text{Aut}}(X)$, consisting of rigid motions *and* reflections. We have $\widetilde{G}/G = \{1, \tau\}$, where τ is some orientation-reversing reflection. One can conclude then that $\#\widetilde{G} = 4! \cdot 2 = 48$. One could write $\tau = -I_3$, the orientation-reversing identity. Thus $g\tau = \tau g \; \forall g \in \widetilde{G}$.   *9/13/24*

It's tempting to say $\widetilde{G} \cong S_4 \times \mathbb{Z}2$, given the construction above, and that $\widetilde{G} = G \sqcup \tau G$. This is correct: take $S_4 \times \mathbb{Z}2 \to \widetilde{G} : (g, i) \mapsto g\tau^i$. We verify this is a homomorphism: $g_1\tau^{i_1}g_2\tau^{i_2} = g_1g_2\tau^{i_1+i_2}$.

The *center* of G, notated $Z(G)$, is $\{z \in G : zg = gz \forall g \in G\}$. Elements in the center   DEF 1.12
are their own conjugations.

Let $\sigma \in S_n$ be decomposed into disjoint cycles $\tau_1, ..., \tau_k$. The unordered set   DEF 1.13
$\{|\tau_1|, ..., |\tau_k|\}$ is called the *cycle shape* of σ. Alternatively, the cycle shape is the partition of n

$$|\tau_1| + ... + |\tau_k| = n$$

where we include all identity cycles (i), with size 1.

───────────────────────── ♠ *Examples* ♣ ─────────────────────────   E.G. 1.5

1. Let $\sigma \in S_n$ fix all elements. Then the cycle shape of σ is dictated by $1 + ... + 1 = n$.

2. Let $\sigma = (1\ 2\ ...\ n) \in S_n$. The cycle shape of σ is dictated by n.

3. Consider all permutations in S_4, decomposed into disjoint cycles. We have

the following cycle shapes:

partition	$\sigma \in S_4$	#
$1 + 1 + 1 + 1$	$\{\mathbb{1}\}$	1
$2 + 1 + 1$	$\{(12), (13), (14), (23), (24), (34)\}$	$\binom{4}{2} = 6$
$3 + 1$	$\{(123), (124), (132), (134), (142), (143), (243), (342)\}$	$4 \cdot 2 = 8$
$2 + 2$	$\{(12)(34), (13)(24), (14)(23)\}$	3
4	$\{(1234), (1243), (1324), (1342), (1423), (1432)\}$	$3! = 6$

1.5 Relation Between Cycle Shape and Conjugation

Two permutations in S_n are conjugate $\iff$ they have the same cycle shape.

PROOF.

($\implies$) Let $g \sim g'$, i.e. $g' = hgh^{-1}$ for some $h \in G$. Let $g(i) = j$. Then $g'(h(i)) = hgh^{-1}h(i) = hg(i) = hj$. Thus, for a disjoint cycle τ of g, say $(a, b, ..., z)$, we have that $\tau' = (h(a), h(b), ..., h(z))$ is a disjoint cycle of g', i.e. they have the same cycle shape.

Let $g, g' \in S_n$ have the same cycle shape. Then consider $h \in S_n$ which permutes the elements of cycles in g to the elements of cycles in g'. Then $hgh^{-1} = g'$.

For example, $g = (123)(45)(6)$ and $g' = (615)(24)(3)$. h is then (163524). $\square$

E.G. 1.6

───────────── ♠ *Examples* ♣ ─────────────

We'll revisit example (3) from above:

conjugacy class	#
$\mathbb{1}$	1
(12)	$\binom{4}{2} = 6$
(123)	$4 \cdot 2 = 8$
$(13)(24)$	3
(1234)	$3! = 6$

Recall that $S_4 \cong \text{Aut(cube)}$. Thus, we may associate each of these conjugacy

classes with conjugacy classes of cube automorphisms:

conjugacy class	#	Aut(cube)
$\mathbb{1}$	1	Id
(12)	$\binom{4}{2} = 6$	rotations about edge diagonals by π
(123)	$4 \cdot 2 = 8$	rot'n about face centers by π
(13)(24)	3	rot'n about principal diagonals by $\frac{\pi}{3}$
(1234)	$3! = 6$	rot'n about face centers by $\frac{\pi}{2}$

Recall Lagrange's Theorem, which states that, for all $H < G$, $|H| \mid |G|$. Is the converse true? Not necessarily (try considering subgroup of order 15 of S_5).

SYLOW THEOREMS

> **1.6   Sylow 1**
>
> Let p be prime. If $\#G = p^t m$, $p \nmid m$, then G has a subgroup of cardinality p^t.

If $H \subseteq G$ is as in <u>Thm 1.7</u>, then H is called a *Sylow p-subgroup* of G.   DEF 1.14

———————————————— ♠ *Examples* ♣ ————————————————   E.G. 1.7

1. $\#S_5 = 120 = 2^3 \cdot 3 \cdot 5$. We can thus find Sylow subgroups of cardinality 8, 3, and 5.

2. $\#S_6 = 720 = 2^4 \cdot 3^2 \cdot 5$. We can find Sylow subgroups of cardinality 16, 9, and 5. The subgroup with 9 elements can be constructed by taking $\langle (123), (456) \rangle$, the generator of two order 3 elements. This is isomorphic to $\mathbb{Z}3 \times \mathbb{Z}3$. What about the subgroup of 16 elements? Take $H = D_8 \times S_2$, where D_8 acts on vertices 1, 2, 3, 4, and S_2 swaps the remaining 5, 6 independently.

3. $\#S_8 = 2^7 \cdot 3^2 \cdot 5 \cdot 7$. How can we find a subgroup with $2^7 = 128$ elements? An idea would be taking $D_8 \times D_8$, and then swapping these squares via S_2, i.e. $H = D_8 \times D_8 \times S_2$.

Take this with a grain of salt, I'm not sure that it works
-Prof. Darmon

Given a prime p and a group G, the following are equivalent: PROP 1.9

1. $\exists$ a G-set of cardinality prime to p, i.e. not a multiple of p, with no orbit of size 1.

2. $\exists$ a transitive G-set of cardinality ≥ 2 and prime to p.

3. G has a proper subgroup of index prime to p.

PROOF.

($1 \implies 2$) Write $X = X_1 \sqcup X_2 \sqcup ... \sqcup X_k$ for orbits X_i. This orbits are especially transitive. Then $\exists j$ such that $|X_j|$ is prime to p. Suppose otherwise. Then $|X| = |X_1| + ... + |X_k| = mp$, so $|X|$ is not prime to p.

($2 \implies 3$). Let X be a transitive G set with $|X| \geq 2$ and $|X|$ prime to p. Then $X \cong G/\text{stab}(x_0)$ for some $x_0 \in X$. If $\text{stab}(x_0) = G \forall x_0 \in X$, then $X = \{\star\}$, i.e. does not have cardinality ≥ 2. Thus, $\text{stab}(x_0) < G$ is a proper subgroup.

($3 \implies 1$). Take $H < G$, a proper subgroup of index prime to p, and consider the G-set $X = G/H$. If X had an orbit of size 1, say of x_0, then $H \sim \text{stab}(x_0) = G$, i.e. is not a proper subset. $\qquad\square$

PROP 1.10

For a finite group G, with $\#G = p^t m$ for some prime p and $m \neq 1$, then (G, p) satisfies Prop 1.9.

PROOF.

Let $X = \{\text{set of } H \subseteq G : \#H = p^t\}$. Then if $A \subseteq X$, $gA \in X$, since $ga = gb \implies a = b$, i.e. g acts faithfully. Furthermore, unless $g = \mathbb{1}$, $A \neq gA$. Thus, X has no fixed points, and thus no orbits of size 1. X therefore (almost) satisfies (1) of Prop 1.9. It remains to show that $|X|$ is prime to p.

$$\#X = \binom{p^t m}{p^t} = \frac{(p^m)(p^m - 1) \cdot ... \cdot (p_t m - p^t + 1)}{p^t \cdot (p^t - 1) \cdot ... \cdot 1}$$

$$= \prod_{j=0}^{p^t - 1} \frac{p^t m - j}{p^t - j}$$

From here, one can show that the maximal power of p dividing the numerator is the same maximal power of p which divides the denominator. Thus, p cannot divide any of the product terms. By Euler's Lemma, then, p cannot divide $\prod$. $\qquad\square$

PROOF OF SYLOW 1

Fix a prime p. Let G be a finite group of minimal cardinality for which Sylow 1 fails (such a group exists: we have found such groups in Example 1.7). By Prop 1.10, (G, p) satisfies (3) of Prop 1.9. Thus, $\exists H < G$ such that $p \nmid [G : H]$. But also, $\#H | \#G$, so $\#H = p^t m_0$ for $m_0 < m$.

By strong induction, $\exists N < H$ of cardinality p^t. N is thus also a p-Sylow subgroup of G, violating minimality $\lightning$. $\qquad\square$

PROP 1.11

If $\#G = p^t m$, with $p \nmid m$, then G has a proper subgroup H of cardinality $p^t m_0 : m_o < m$.

PROOF.

This is mentioned in the previous proof. By (3) of Prop 1.9, we have a proper subgroup $H < G$ with $p \nmid \frac{p^t m}{\#H}$ and $\#H | p^t m$.

Thus, $\#H = p^{t_0} m_0$ with $t_0 \le t, m_0 \le m$. If $t_0 < t$, then

$$p \nmid \frac{p^t m}{p^{t_0} m_0} = p^{t-t_0} \frac{m}{m_0} \lightning$$

$\implies t_0 = t$. Then, if $m_0 = m$, $H = G$, but H is proper.

$\implies \#H = p^t m_0 : m_0 < m.$ $\qquad\square$

<div style="text-align:right">PROP 1.12</div>

If G is abelian and finite, with $p | \#G$ for a prime p, then G has an element of order p. Thus G has a subgroup of order p.

<div style="text-align:right">PROOF.</div>

Let $\#G = pm$. It is sufficient to find $g \in G$ with $p | \mathrm{ord}(g)$, since then $\mathrm{ord}(g^{\frac{\mathrm{ord}(g)}{p}}) = p$. Let $g_1, ..., g_t \in G$ be the set of generators for G. Let $n_i = \mathrm{ord}(g_i)$. Then consider the homomorphism

$$\varphi : n_1 \mathbb{Z} \times ... \times n_t \mathbb{Z} \to G : (a_1, ..., a_t) \to g_1^{a_1} \cdot ... \cdot g_t^{a_t}$$

This is surjective, since we can always write $g \in G$ in terms of powers of generators. Recall that, for a homomorphism $\varphi : A \to B$, $A/\ker(\varphi) \cong \mathrm{Im}(\varphi)$. Thus, $\#G | n_1 \cdot ... \cdot n_t$. But $p | \#G \implies p | n_1 \cdot ... \cdot n_t \implies p | n_j$ for some j. Then $p | \mathrm{ord}(g_j)$. $\qquad\square$

1.7 Sylow 2

If H_1, H_2 are Sylow$-p$ subgroups of G, then $\exists g \in G$ with $g H_1 g^{-1} = H_2$.

<div style="text-align:right">PROOF.</div>

Let $\#G = p^t m : p \nmid m$. Let H_1, H_2 have cardinality p^t. Consider G/H_1 as a G-set. In fact, think of G/H_1 as an H_2-set. Then we may decompose into orbits:

$$G/H_1 = X_1 \sqcup X_2 \sqcup ... \sqcup X_N$$

Then $\#X_i | \#H_2$ by Orbit-Stabilizer, so $\#X_i = p^a : a \le t \; \forall i$. Then $\exists$ an orbit of size 1, otherwise $p | G/H_1 \implies p | m \lightning$.

Let $X_j := \{g H_1\}$. Thus, $\forall h \in H_2, hg H_1 = g H_2 \implies g^{-1} hg \in H_1$, i.e. $\exists g : g^{-1} H_2 g = H_1$. Rewriting, this means $g H_1 g^{-1} = H_2$. $\qquad\square$

Given a group G and $H < G$, we call $\{g \in G : g H g^{-1} = H\}$ the *normalizer* of H.

<div style="text-align:right">DEF 1.15</div>

H is a subgroup of its normalizer.

<div style="text-align:right">PROP 1.13</div>

<div style="text-align:right">PROOF.</div>

$\varphi : H \to H : h \mapsto ghg^{-1}$, where $g \in H$, is a bijection (check for yourself). Thus, $gHg^{-1} = H$ for a fixed $g \in H$, so $H < N$, the normalizer of H. $\qquad \square$

> ### 1.8 Sylow 3
>
> Let N_p be the number of distinct Sylow-p subgroups of G. Then
>
> 1. $N_p | m$, where $\#G = p^t m : p \nmid m$
>
> 2. $N_p \equiv 1 \mod p$

PROOF.

(1st Claim) Let X be the set of Sylow-p subgroups, and consider X as a G-set under conjugation. By Sylow 2, X is transitive. Thus, $X \cong G/\text{stab}(H) \; \forall H \in X$. Fix some H. Notice that $\text{stab}(H)$ is the normalizer of H. Thus, $\#H | \#\text{stab}(H) \implies \#G/\#\text{stab}(H) | \#G/\#H = \frac{p^t m}{p^t} = m$. We conclude that $\#X | m$.

(2nd Claim) Let H be a Sylow-p subgroup. Let X be the set of all Sylow-p subgroups, viewed as an H-set by conjugation. We decompose X into orbits:

$$X = X_1 \sqcup X_2 \sqcup \ldots \sqcup X_a$$

X_i are all transitive, so $\#X_i | \#H = p^t \implies \#X_i = 1 \vee p \vee \ldots \vee p^t$. We claim that there is exactly one orbit of size 1. Let $X_j = \{H'\}$ be an orbit of size 1. Then $aH'a^{-1} = H' \; \forall h \implies H$ is a subset of the normalizer of H'. Let $H \subseteq R = \{a \in G : aH'a^{-1} = H'\}$. Then H' is a normal subgroup of R. Thus, we may consider R/H' as a group. Then $\frac{\#R}{\#H'} = \frac{\#R}{p^t} = \frac{p^t m_0}{p^t} = m_0 < m \implies p \nmid \frac{\#R}{\#H'}$.

Consider the natural map $\varphi : R \to R/H'$. Then $\#\varphi(H) | p^t$ (by First Iso. Thm.) and also $\#\varphi(H) | \frac{\#R}{\#H'}$ (by Lagrange). But $p \nmid \frac{\#R}{\#H'}$, so $\#\varphi(H) = 1$. Then $H \subseteq \ker(\varphi) = H'$, but $\#H = \#H'$, so $H = H'$. We could always have chosen H as an orbit of size 1, and find now that all other orbits of size 1 are exactly H. Thus, $|X| = N_p \equiv 1 \mod p$. $\qquad \square$

PROP 1.14

If p, q are primes with $p < q$ and $p \nmid q - 1$, then all groups of cardinality pq are cyclic.

BURNSIDE'S LEMMA

DEF 1.16

Let G be a group, and let X be a G-set. Given $g \in G$, we consider $X^g := \{x \in X : gx = x\}$. Denote by $\text{FP}_X(g) = \#X^g$.

For instance, if $G = S_4$ with $X = \{1, 2, 3, 4\}$, then $X^{(12)} = \{3, 4\}$. Thus, $\text{FP}_X((12)) = 2$. Consider also $\text{FP}_X((12)(34)) = 0$.

PROP 1.15

$\text{FP}_X(hgh^{-1}) = \text{FP}_X(g) \; \forall h \in G$.

PROOF.

Take the bijection $\varphi : X^g \to X^{hgh^{-1}}$ by $\varphi(x) = hx$.   □

1.9   Burnside's Lemma

$$\frac{1}{\#G} \sum_{g \in G} \mathrm{FP}_X(g) = \#(X/G) = \#\text{orbits of } X$$

Let $\Sigma \subseteq G \times X$ be $\Sigma = \{(g, x) : gx = x\}$. We'll count Σ in two ways: PROOF.

1. $\Sigma = \sum\limits_{g \in G} \mathrm{FP}_X(g)$ by definition

2. $\Sigma = \sum\limits_{x \in X} \#\mathrm{stab}(x) = \sum\limits_{O \in X/G} \sum\limits_{x \in O} \#\mathrm{stab}(x)$. By Orbit-Stabilizer, $\#\mathrm{stab}(x)\#O = \#G$, where $x \in O$. Thus, we have

$$\Sigma = \sum_{O \in X/G} \sum_{x \in O} \frac{\#G}{\#O} = \sum_{O \in X/G} \#G = \#(X/G)\#G$$

Thus, $\sum\limits_{g \in G} \mathrm{FP}_X(g) = \#(X/G)\#G$ as desired.   □

If X is a transitive G-set, with $|X| > 1$, then $\exists g \in G$ such that $\mathrm{FP}_X(g) = 0$.   PROP 1.16

If X is transitive, then, by Burnside, $\sum\limits_{g \in G} \mathrm{FP}_X(g) = \#G$. But $\mathrm{FP}_X(\mathbb{1}) = \#X > 1$.   PROOF.

Thus, $\sum\limits_{g \in G \setminus \mathbb{1}} \mathrm{FP}_X(g) \leq \#G - 2$. The result follows by pigeonhole principle.   □

Let $C = \{1, ..., t\}$. A coloring of X by C is a function $X \to C$. The set of such   DEF 1.17
functions we denote by C^X. Note that $|C^X| = |C|^{|X|}$.

EXCEPTIONAL OUTER AUTOMORPHISM OF s_6

All automorphisms on S_n are typically *inner*, i.e. can be written instead as
a conjugation by some element. However, in S_6 there exists a unique *outer*
automorphism, i.e. one which is not inner. Thus, we call it *exceptional*.

We are able to find an S_5-set of cardinality 6 (this comes from considering S_5/F_{20},
where F_{20} is the Frobenius group of 20 elements). Thus, one constructs the group
action homomorphism $\varphi : S_5 \to \mathrm{Aut}(X)$, and finds the subgroup $\varphi(S_5) \cong S_5 \subseteq S_6$.
We also have the typical subgroup $\mathrm{stab}(i) \cong S_5 \subseteq S_6$. Importantly, these two
subgroups are not conjugate to eachother. Denote $\mathrm{stab}(i) = S_5$ and $\varphi(S_5) = \widetilde{S_5}$.

$$S_5 \subset S_6 \supset \widetilde{S_5}$$

To investigate the outer automorphism of S_6, we first consider the cycle shapes in F_{20} (i.e. conjugation classes of F_{20}). They are as follows:

$$(1234) \qquad (12)(34) \qquad (12345)$$

Similarly, in S_5, we have

Shape	Name	#	on S_5/F_{20}
$\mathbb{1}$	$1A$	1	$\mathbb{1}$
(12)	$2A$	10	$(12)(34)(56)$
$(12)(34)$	$2B$	15	$(12)(34)$
(123)	$3A$	20	$(123)(456)$
(1234)	$4A$	30	(1234)
(12345)	$5A$	24	(12345)
$(12)(345)$	$6A$	20	(123456)

For $2A$: Note that F_{20} has no transpositions, so $2A$ will have no fixed points. Thus, consider order 2 permutation on 6 elements with no fixed points: there is only $(12)(34)(56)$.

For $4A$: How many fixed points does $4A$ have in S_5/F_{20}? It must have some, since the shape (1234) appears in F_{20}. Thus, we have an order 4 element in S_6 which fixes some points. This is only (1234).

For $2B$: We know that $2A = 4A^2$, so $2A$ will look like $(12)(34)$.

For $3A$: There are no 3 cycles in F_{20}, so this has no fixed points in S_5/F_{20}. There is one such permutation on 6 elements, $(123)(456)$

For $5A$: There is only one order 5 cycle on 6 elements, and that is (12345).

For $6A$: Since $(12)(345)$ is not in F_{20}, we observe no fixed points in S_5/F_{20}. There is only one such permutation on 6 elements of order 6, and that is (123456).

Thus, we conclude that $\widetilde{S_5} \subseteq S_6$, which is constructed via the action of S_5 on S_5/F_{20}, has exactly the cycle shapes expressed in the right-most column.

Now we investigate the cycle shapes in S_6:

Shape	Name	#	on $S_6/\widetilde{S_5}$
$\mathbb{1}$	$1A$	1	$\mathbb{1}$
(12)	$2A$	15	(12)(34)(56)
(12)(34)	$2B$	45	(12)(34)
(12)(34)(56)	$2C$	15	(12)
(123)	$3A$	40	(123)(456)
(123)(456)	$3B$	40	(123)
(1234)	$4A$	90	(1234)
(1234)(56)	$4B$	90	(1234)(56)
(12345)	$5A$	144	(12345)
(123456)	$6A$	120	(123)(45)
(123)(45)	$6B$	120	(123456)

<u>For $2A$:</u> Since $\widetilde{S_5}$ contains no single transpositions, $2A$ on $S_6/\widetilde{S_5}$ will have no fixed points. There is one such permutation of order 2, then, which is (12)(34)(56).

An automorphism $\varphi : G_1 \to G_2$ will send conjugacy classes of G_1 to conjugacy classes of G_2. Thus, for a conjugacy classes C_1 of G_1, $\varphi(C_1)$ is a conjugacy class of G_2 of equal cardinality.

PROP 1.17

<u>For $2B$:</u> We map to a conjugacy class of order 2 elements of size 45 to another of size 45. Thus, there is only (12)(34).

<u>For $2C$:</u> By pigeonhole, we can map only to the remaining conjugacy class of order 2 elements, (12).

<u>For $3A$:</u> We do not have (123) in $\widetilde{S_5}$, so we have no fixed points on $S_6/\widetilde{S_5}$. The only order 3 cycle satisfying this is (123)(456).

<u>For $3B$:</u> By pigeonhole, we map to (123).

<u>For $4A$:</u> We have fixed points on $S_6/\widetilde{S_5}$, since (1234) $\in \widetilde{S_5}$. Thus, we map to (1234).

<u>For $4B$:</u> By pigeonhole, we map to (1234)(56).

<u>For $5A$:</u> We have only one order 5 cycle to choose from, and that is (12345).

<u>For $6A$:</u> The cycle (123456) is in $\widetilde{S_5}$, so we act on $S_6/\widetilde{S_5}$ with some fixed points. The only order 6 cycle satisfying this is (123)(45).

<u>For $6B$:</u> By pigeonhole, we map to (123456).

IDENTIFYING NORMAL SUBGROUPS

Given G, how might we identify its normal subgroups? We'll proceed by example. $G = A_5$, with $\#A_5 = 60$. We know that A_5 has no non-trivial normal subgroups. How can we show this?

One computes the conjugacy classes their sizes of G:

Shape	Name	#
$\mathbb{1}$	$1A$	$\mathbb{1}$
$(12)(34)$	$2A$	15
(123)	$3A$	20
(12345)	$5A$	24

However, in A_5, $24 \nmid 60$, so $5A$ is *not* in fact a conjugacy class. Consider $X = (12345)^{A_5}$, all conjugations of $5A$. This is, by definition, a transitive A_5-set. Invoking Orbit Stabilizer, $|X| = \frac{\#A_5}{\#\mathrm{stab}(12345)}$. Then, the stabilizer of (12345) is

$$H := \{g \in A_5 : g(12345)g^{-1} = (12345)\} = \{g \in A_5 : g(12345) = (12345)g\}$$

Clearly any power $(12345)^j$ is in H for $j = 1, 2, 3, 4, 5$. We can further identify $\{1, 2, 3, 4, 5\}$ with $\mathbb{Z}5$, and observe that $\delta(x) = (12345)(x) = x + 1 \mod 5$. So we'd like $g\delta(j) = \delta(j)g \implies g(j+1) = g(j) + 1$. Thus, if $g(1) = a$, then $g(2) = a + 2$, etc., etc. Thus, we can find only 5 such δ, so indeed $H = \{(12345)^j : j \in [1, 5]\}$, and $\#X = \frac{60}{5} = 12$.

Thus, we correct our prior statement and write that $\#5A = 12$. But (12345) is not conjugate to (12354) in A_5 (a transposition runs between them), so in fact we have two conjugacy classes of 5 cycles.

Shape	Name	#
$\mathbb{1}$	$1A$	$\mathbb{1}$
$(12)(34)$	$2A$	15
(123)	$3A$	20
(12345)	$5A$	12
(12354)	$5B$	12

PROP 1.18

A normal subgroup is a union of conjugacy classes.

The divisors of 60 are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30. We can rule out 1, ..., 12, since no conjugacy class is small enough to contain these. We must include the identity, so 15 is too small as well. For 20 and 30, by considering combinations, we cannot partition with the classes above.

MIDTERM 2023 Q4

Let n be odd. Let P be a Sylow-2 subgroup of S_{n-1}. Then P acts on $\{1, ..., n-1\}$ without fixed points (else, P would be isomorphic to a subgroup of S_{n-2}—but $2 \nmid n - 2$). Thus P lies in S_n by fixing exactly one element. We may choose n such elements, and thus n such copies of $S_{n-1} \subset S_n$.

II   Rings & Fields

FIRST PROPERTIES

People developed rings by counting: 0, 1, 2, 3, ... are natural. We generalize:

A *ring* is a set R endowed with two binary operations, denoted $+$ and $\times$, such that   DEF 2.1
$+, \times : R \times R \to R$. The following axioms govern rings:

1. The neutral element $\mathbb{0}$ is such that $a + \mathbb{0} = a \; \forall a \in R$.

2. The inverse of a, denoted $(-a)$, is such that $a + (-a) = \mathbb{0}$.

3. The neutral element $\mathbb{1}$ is such that $a \times \mathbb{1} = a \; \forall a \in R$.

4. R is associative over (strictly) addition and multiplication

5. We have the following two distributive laws:

    (a) $a \times (b + c) = a \times b + a \times c$.
    (b) $(b + c) \times a = b \times a + c \times a$.

Notes on rings: PROP 2.1

1. We denote by $(R, \cdot)$ the ring R endowed only with only the operation $\cdot$. Then, $(R, +)$ is an abelian group. We call $(R, \times)$ a *monoid*.

2. Sometimes, we do not require $\mathbb{1}$ (take the ring of even numbers, which has no units). However, in this class we will always have $\mathbb{1}$.

3. $\mathbb{1} \neq \mathbb{0}$ (i.e. we do not consider the zero ring).

4. $\mathbb{0}$ is never invertible, and $\mathbb{0}a = \mathbb{0} \; \forall a$.

5. $(-a) \times (-b) = ab$

─────────────────────── ♠ *Examples* ♣ ───────────────────────   E.G. 2.1

1. $\mathbb{Z}$ is a ring.

2. $\mathbb{Q} = \{\frac{a}{b} : b \neq 0\}$, with $+, \times$, is a ring. We may complete $\mathbb{Q}$ by taking {Cauchy sequences}/{null sequences} $= \mathbb{R}$

3. Given a prime p, $|x - y|_p = p^{-\mathrm{ord}_p(x-y)}$. $x - y = \Pi q^{e_q} : e_q \in \mathbb{Z}$. Then $\mathrm{ord}_p(x - y) = e_p$. Note that $|ab|_p = |a|_p|b|_p$, and $|a + b|_p \leq |a|_p + |b|_p$. The completion by this metric is denoted $\mathbb{Q}_p$ (the field of p-atic numbers).

4. $\mathbb{C} = \mathbb{R}[i] = \{a + bi : a, b \in \mathbb{R}\}$.

Recall completion in the analysis sense: X is not complete if it has a Cauchy sequence which does not converge in it; then the completion of X is $X \cup \{$limits of Cauchy seq's$\}$

5. $R[x] = \{a_0 + a_1 x + \ldots + a_n x^n : a_i \in \mathbb{R}\}$.

6. $R \leftrightarrow \#$ line and $\mathbb{C} \leftrightarrow$ plane geometry. For the latter, we note the properties

$$a + bi = r_1 e^{i\theta_1} \qquad c_1 \cdot c_2 = r_1 r_2 e^{i(\theta_1 + \theta_2)}$$

Q: is there a ring which may be well adopted to $\mathbb{R}^3$ geometry? **A:** No, not quite. It is possible to do so with $\mathbb{R}^4$ 👎. From this arises the Hamilton quaternions:

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\} \qquad i^2 = j^2 = k^2 = -1$$

with $ij = -ji = k, jk = -kj = i, ik = -ki = j$.

7. Let R be some commutative ring. Then $M_n(R) = n \times n$ matrices with entries on R. $M_n(R)$ is a ring, where $\mathbb{0}$ is the matrix with all 0 entries, and $\mathbb{1}$ is the matrix with all 0 entries except on the diagonal (where they are 1).

   Showing $(AB)C = A(BC)$ is tough via brute-force, but easy when taking an isomorphism from $M_n(R)$ to linear transformations on $R \to R$, with $M_1 M_2 \to f_1 \circ f_2$.

8. We may take a ring $R \rightsquigarrow (R, +, \mathbb{0})$, an additive, commutative group. Similarly, $R \rightsquigarrow (R^\times, \times, \mathbb{1})$, which is an associative multiplicative group. We denote by $R^\times$ the set of units in R, i.e. $\{a \in R : \exists a' : aa' = a'a = \mathbb{1}\}$.

DEF 2.2

A ring R such that $r_1 r_2 = r_2 r_1 \forall r_1, r_2 \in R$ is called *commutative*.

DEF 2.3

A *homomorphism* of rings, $\varphi : R_1 \to R_2$ is such that

$$\varphi(a + b) = \varphi(a) + \varphi(b) \qquad \varphi(ab) = \varphi(a)\varphi(b) \qquad \forall a, b \in R_1$$

From this arises the property $\varphi(\mathbb{1}_{R_1}) = \mathbb{1}_{R_2}$. Alternatively, φ is a ring homomorphism if it is an additive group homomorphism and obeys $\varphi(ab) = \varphi(a)\varphi(b)$.

DEF 2.4

It is tempting to consider elements sent to 1, as in group kernels; however, *this* kernel will not be closed under multiplication, and is hence less interesting to study.

The *kernel* of φ, denoted $\ker(\varphi)$, is the set

$$\{a \in R_1 : \varphi(a) = 0\}$$

Recall that, in groups, $\ker(\varphi)$ is normal, and every normal subgroup may be conceptualized as the kernel of some group homomorphism. We have a similar notion in rings:

DEF 2.5

Note, if R is commutative, we only need to check one of these inclusions.

$I \subseteq R$ is called an *ideal* if

1. I is an additive subgroup of R

2. $\forall r \in R, ri \in I, ir \in I$

PROP 2.2

If φ is a ring homomorphism, then $\ker(\varphi)$ is an ideal.

PROOF.

Condition (1) follows from the fact that φ is an additive group homomorphism. Condition (2) follows from $\varphi(ri) = \varphi(r)\varphi(i) = \varphi(r) \cdot 0 = 0$, and similarly for $\varphi(ir) = 0$. $\qquad \square$

If $I \subseteq R_1$ is an ideal, then $\exists$ a ring R_2 and a homomorphism $\varphi : R_1 \to R_2$ such that $\ker(\varphi) = I$. PROP 2.3

Consider $R_2 := R_1/I = \{a + I : a \in R_1\}$. Since I is commutative as an additive ring, it is normal, and thus R_1/I is a group under addition. For multiplication, we define $(a+I)(b+I) = (ab+I)$. Then let $\varphi : R_1 \to R_1/I$ be such that $a \mapsto a+I$. $\ker(\varphi) = \{a \in R_1 : a + I = I\} = \{a \in R_1 : a \in I\} = I$. PROOF. $\qquad \square$

Note that $\mathbb{0}_{R/I} = 0 + I$ and $\mathbb{1}_{R/I} = 1 + I$.

2.1 First Isomorphism Theorem

Let R be a ring (or a group), and let φ be a surjective ring (or group) homomorphism. Then $\mathrm{Im}(\varphi) \cong R/\ker(\varphi)$.

We may take $\mathrm{Im}(\varphi) \to R/\ker(\varphi) : a \mapsto \varphi^{-1}(a)$ and $R/\ker(\varphi) \to \mathrm{Im}(\varphi) :$ $a + \ker(\varphi) \mapsto \varphi(a)$. One can show without too much trouble that these are homomorphisms and inverses of eachother, and thus bijective. PROOF. $\qquad \square$

An *ideal* $I \subseteq R$ is called *maximal* if it is not properly contained in any proper ideal of R, i.e. $I \subsetneq I' \implies I' = R$ for any ideal I'. DEF 2.6

An ideal $I \subseteq R$ is called *prime* if $ab \in I \implies a \in I$ or $b \in I$. DEF 2.7

Let $R = \mathbb{Z}$, $I = n\mathbb{Z} = (n) = \{na : a \in \mathbb{Z}\}$. Then (n) is prime $\iff n$ is prime. PROP 2.4

($\impliedby$) If $ab \in (n)$, then $n|ab$. By Gauss' Lemma, $n|a$ or $n|b$. Thus, $a \in (n)$ or $b \in (n)$. PROOF.

($\implies$) By contrapositive: let $n = ab$. Then $ab \in (n)$. But $a, b < n$, so $a, b \notin (n)$. $\qquad \square$

2.2 Integers are Principal

If $I \subseteq Z$ is an ideal, then $\exists n \in \mathbb{Z}$ such that $I = (n)$.

PROOF.

Proof 1. Consider the quotient $\mathbb{Z}/I$. As an abelian group, it is cyclic, generated by $1 + I$. Let $n := \#(\mathbb{Z}/I) = \text{ord}(1 + I)$. If $n = \infty$, then $\mathbb{Z} \to \mathbb{Z}/I$ is injective, so $I = (0)$. Otherwise, $I = (n)$.

Proof 2. Assume that $I \neq (0)$. Let $n = \min\{a \in I : a > 0\}$. Let $a \in I$. Then $a = qn + r$, where $0 \leq r \leq n$. Then $a \in I, n \in I, qn \in I$ (by sucking in), so $a - qn \in I$. Thus, $r \in I \implies r = 0$ by minimality. $\qquad\square$

DEF 2.8

Let R be a commutative ring. An ideal of the form $aR = (a) = \{ar : r \in R\}$ is called a *principal ideal*.

DEF 2.9

A ring in which every idea is principal is called a *principal ideal ring*.

> ### 2.3   Polynomials are Ideal
>
> Consider $R = \mathbb{F}[x]$, where $\mathbb{F}$ is a field. If I is an ideal of $\mathbb{F}[x]$, then I is principal

By convention, we say $\deg(0) = -\infty$ in order to satisfy $\deg f(x)g(x) = \deg f(x) + \deg g(x)$. Note that $\deg(c) = 0$ where $c \neq 0$.

PROOF.

Let $f(x)$ be a polynomial in I of minimal degree (with $I \neq (0)$). Then let $\deg f(x) = d$, where $d \leq \deg g(x) \; \forall g \in \mathbb{F}[x]$.

For $g(x) \in I$, we may write $g(x) = f(x)q(x) + r(x)$, where $\deg r(x) < d$. Then $r(x) \in I$ by the same arguments presented in Thm 2.2. Thus, $\deg r(x) = 0$, so $I = (f)$. $\qquad\square$

E.G. 2.2

──────────────── ♠ *Examples* ♣ ────────────────

1. Let $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, and let $I = \{a + n\mathbb{Z}\}$ be some ideal of $\mathbb{Z}/n\mathbb{Z}$. Then $\varphi^{-1}(I)$ is an ideal of $\mathbb{Z}$. Hence, $\varphi^{-1}(I) = (a)$ for some $a \in \mathbb{Z}$.

2. Let $R = \mathbb{Z}[x]$. Then $I = \{f(x) : f(0) \text{ is even}\} \subsetneq \mathbb{Z}[x]$. We claim that I is an ideal. We know that I is an additive subgroup of $\mathbb{Z}[x]$. If $f(x) \in \mathbb{Z}[x]$, $g(x) \in I$, then $f(x)g(x) \in I$, since $f(0)g(0)$ is always even.

3. If I were of the form $a\mathbb{Z}[x]$, then $a|2$ and $a|x$, so $a = \pm 1$. But $I \subsetneq \mathbb{Z}[x]$, so this can't be the case. From this example we consider $I = (2, x) = 2\mathbb{Z}[x] + xZ[x]$. This is not principal.

4. Let $R = \mathbb{F}[x, y]$ (a polynomial ring of two variables). Consider $(x, y) = Rx + Ry$. Note that all elements in this ideal are non-constant. We may write $Rx + Ry = \{f(x, y) : f(0, 0) = 0\}$.

──

PROP 2.5

I is a prime ideal of R if and only if R/I has no zero divisors (i.e. $\exists x, y \neq 0 : xy = 0$).

DEF 2.10

A ring which satisfies this is called an *integral domain*.

PROOF.

($\implies$). Given $a + I, b + I \in R/I$, let $(a + I)(b + I) = 0$. Then $ab + I = 0$, so $ab \in I$. Then $a \in I$ or $b \in I$, i.e. $a + I = 0$ or $b + I = 0$. Thus, R/I has no zero divisor.
$\square$

If R is an integral domain, then it satisfies the cancellation law:

$$\forall a \neq 0, ax = ay \implies x = y$$

I is a maximal ideal $\iff R/i$ is a field.

($\implies$)$a + I \in R/I$. If $a + I \neq 0$, then $Ra + I \supsetneq I$. By maximality, $Ra + I = R$. Then, let $b \in R, i \in I$. We have $1 = ba + i \implies 1 + I = (b + I)(a + I) \implies (b + I) = (a + I)^{-1}$.

($\impliedby$) Given an ideal $J \supsetneq I$, let $a \in J - I$. Then $a + I \neq 0$. Thus, $\exists b$ such that $ba + I = 1 + I$ in R/I, since it is a field. Thus, $1 \in J \implies R = J$. (By absorption property).
$\square$

I is prime $\iff R/I$ is an integral domain.

QUOTIENTS

$R/I, a + I = b + I \iff a - b \in I$. If $I = (d)$, then $a + I = b + I \iff d|(b - a)$.

———————————————————— ♠ *Examples* ♣ ————————————————————

1. $R = \mathbb{Z}, I = (n)$. Then $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} : a \in \mathbb{Z}\} = \{0, 1, 2, ..., n - 1\}$†

2. $R = \mathbb{F}[x], I = (f(x))$. Then $\mathbb{F}[x]/(f(x)) = \{p(x) + f(x)\mathbb{F}[x]\} = \{p(x) : \deg(p(x)) \leq d - 1\}$, where $d = \deg(f(x))$†

3. $R = \mathbb{Z}[x], I = (2, x) = \{f(x) : f(0) \text{ even}\}$. Then $\mathbb{Z}[x]/(2, x)$ has two elements: functions where $f(0)$ is even, and functions where $f(0)$ is odd. Thus, $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$.

Consider the homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$ such that $f(x) \mapsto f(0)$ mod 2. This is clearly surjective. Then $\ker(\varphi) = \{f(x) : f(0) \text{ even}\} = (2, x)$. By Thm 2.1, $\mathbb{Z}[x]/\ker(\varphi) \cong \mathbb{Z}/2\mathbb{Z}$, so $\mathbb{Z}[x] \cong \mathbb{Z}/2\mathbb{Z}$.
$\square$

4. $R = \mathbb{F}[x, y], I = (x, y) = x\mathbb{F}[x, y] + y\mathbb{F}[x, y] = \{f(x, y) : f(0, 0) = 0\}$. Then $R/I \cong \mathbb{F}$, with cosets classifying exactly $f(0, 0)$.

Consider $\varphi : f(x, y) + I \mapsto f(0, 0)$, as before.
$\square$

5. $R = \mathbb{F}[x_1, ..., x_n]$, $I = (f_1, ..., f_t)$, where $f_i(x_1, ..., x_n)$ are polynomials of n variables. Finding R/I is difficult. We are touching on algebraic geometry here. Let

$$V(I) = \left\{ \quad (x_1, ..., x_n) \text{ s.t. } \begin{cases} f_1(x_1, ..., x_n) = 0 \\ f_2(x_1, ..., x_n) = 0 \\ \quad \vdots \\ f_t(x_1, ..., x_n) = 0 \end{cases} \right\} \in (\overline{\mathbb{F}})^n$$

The algebraic closure of $\mathbb{F}$.

PROP 2.9

Given a ring R, $p(x) \in R[x]$, there exists a ring $S \supset R$ containing a root of $p(x)$.

PROOF.

Let $S = R[x]/((p(x)))$. Then consider $R \to S$ by $a \mapsto a + (p(x))$. Let $\alpha = x + (p(x))$. Then $p(\alpha) = p(x) + (p(x)) = 0 + (p(x))$. $\qquad \square$

For example, $R = \mathbb{R}$, $p(x) = x^2 + 1$. $R[x]/(x^2 + 1) = \mathbb{C}$.

2.4 Adjustment of Elements

Let $\mathbb{F}$ be a field, and let $f(x) \in \mathbb{F}[x]$ be irreducible. Then $\exists$ a field $K \supset F$ such that K contains a root of $f(x)$.

PROOF.

We let $K = \mathbb{F}[x]/\langle f(x) \rangle$. We wish to show that $\langle f(x) \rangle$ is maximal. Assume otherwise. Then $\langle f(x) \rangle \subseteq I$. But $\mathbb{F}[x]$ is principle, so $\exists g$ with $I = \langle g(x) \rangle$. Then $f(x) = g(x)q(x)$ for some $q(x) \in \mathbb{F}[x]$. But $f(x)$ is irreducible, so $g(x) = \alpha \vee \alpha f(x)$. In the former, we have that $I = \mathbb{F}[x]$. In the latter, we have that $I = \langle f(x) \rangle$. Thus, we conclude that $\langle f(x) \rangle$ is maximal.

Thus, $\mathbb{F}[x]/\langle f(x) \rangle$ is a field. We also need to show that $K \supset \mathbb{F}$, i.e. find an injection between the two. Let $\varphi : \mathbb{F} \hookrightarrow K : \lambda \to \lambda + \langle f(x) \rangle$.

Lastly, we need to show that $f(t)$ has a root in K. We have $f(t) \in \mathbb{F}[t] \subset K[t]$. Let $\alpha \in K := x + \langle f(x) \rangle$. Then $f(\alpha) = f(x + \langle f(x) \rangle) = f(x) + \langle f(x) \rangle = 0$ in K. $\qquad \square$

Generally, for R/I, $f(x) \in \mathbb{R}[x]$, and $a + I \in R/I$, we have $f(a + I) = f(a) + I$. One may show this by induction.

──────────── ♠ *Examples* ♣ ────────────

E.G. 2.4

1. Consider $F = \mathbb{R}$, $x^2 + 1$. Let $\mathbb{C} = \mathbb{R}[x]/\langle x^2 + 1 \rangle$. Concretely, this is $\{a + bx : a, b \in \mathbb{R}\}$ and $x^2 \cong -1 \mod x^2 + 1$.

2. Consider $F = \mathbb{Q}$, $x^2 - 2$. Then $K = \mathbb{Q}[x]/\langle x^2 - 2 \rangle := \mathbb{Q}[\sqrt{2}] = \langle a + b\sqrt{2} : a, b \in \mathbb{Q} \rangle$.

If F is a finite field, then $\#F = p^t$ with p a prime number.   PROP 2.10

> If R is any ring, then there is a unique homomorphism $\varphi : \mathbb{Z} \to R$ which   PROOF.
> sends $0_{\mathbb{Z}} \to 0_R$ and $1_{\mathbb{Z}} \to 1_R$. This same homomorphism applied to F, i.e.
> $\varphi : \mathbb{Z} \to F$, is not injective, since F is finite.
>
> Let $\ker(\varphi) = I$. Then, by the isomorphism theorem, $\overline{\varphi} : \mathbb{Z}/I \to F$ which sends
> $a + I \to \varphi(a)$ is an injection. Thus, we may view $\mathbb{Z}/I$ as a subring of F. Hence,
> $\mathbb{Z}/I$ contains no zero divisors, so it is an integral domain. Hence, by Prop 2.7,
> I is a prime ideal. In $\mathbb{Z}$, this means $I = p\mathbb{Z}$ for some p.
>
> Thus, F contains $\mathbb{Z}/p\mathbb{Z}$. Then F may be viewed as a vector space over $\mathbb{Z}/p\mathbb{Z}$,
> necessarily finite dimensional. Thus, let $t = \dim(F)$. Hence, $F \cong (\mathbb{Z}/p\mathbb{Z})^t$ as a
> vector space isomorphism, so $\#F = p^t$. $\square$

Given a prime p and some t, is there a field of cardinality p^t? If so, how many are
there? If $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ is irreducible of degree t, then we have a candidate for
$\mathbb{Z}/p\mathbb{Z}[x]/\langle f(x) \rangle$ has cardinality p^t.

III   Modules & Vector Spaces

BASES

Just as we can associate $G \rightsquigarrow G$-set, we wish to let rings "act" on something," i.e. $R \rightsquigarrow R$-module.

DEF 3.1   An R-module over R is an abelian group M equipped with a map $R \times M \to M$. Let $\lambda_\times$ and $m_\times$ denote elements in R and M, respectively. Then the map satisfies

1. $\lambda(m_1 + m_2) = \lambda m_1 + \lambda m_2$

2. $\lambda(-m) = -\lambda m$

3. $\lambda \mathbb{0}_M = \mathbb{0}_M$

In other words, $\forall \lambda \in R$, the map $m \mapsto \lambda m$ is a group homomorphism $M \to M$.

4. $(\lambda_1 + \lambda_2)m = \lambda_1 m + \lambda_2 m$

5. $(\lambda_1 \lambda_2)m = \lambda_1(\lambda_2 m)$

6. $\mathbb{1}_R m = m$

DEF 3.2   If M is an abelian group, then the *endomorphism ring* of M is defined as follows:

$$\text{End}(M) = \{f : M \to M : f \text{ is a group homo.}\}$$

$\text{End}(M)$ is a ring under the following operations:

$$(f + g)(m) = f(m) + g(m) \qquad (f \cdot g)(m) = (f \circ g)(m)$$

PROP 3.1   The axioms of Def 3.1 may be reduced to the following: for a ring R and abelian group M, an we say M is an R-module if the operation $R \times M \to M$ defines a ring homomorphism $R \to \text{End}(M)$.

DEF 3.3   If $R = \mathbb{F}$ is a field, then an R-module M is called a *vector space*.

DEF 3.4   Let M be an R-module. A set $\Sigma \subseteq M$ is called a *spanning set* if, for all $m \in M$, $\exists m_1, ..., m_t \in \Sigma$, $\lambda_1, ..., \lambda_t \in R$, with

$$m = \lambda_1 m_1 + ... + \lambda_t m_t$$

Note that we only consider finite linear combinations, even though Σ itself may be infinite.

DEF 3.5   An R-module M is called *finitely generated* if it admits a finite spanning set.

DEF 3.6 $\Sigma \subseteq M$ is said to be *linearly independent* if, $\forall m_1, ..., m_t \in \Sigma$ and $\lambda_1, ..., \lambda_t \in R$,

$$\lambda_1 m_1 + ... + \lambda_t m_t \implies \lambda_1 = ... = \lambda_t = 0$$

$\Sigma \subseteq M$ is a *basis* if it is a spanning set and is linearly independent.   DEF 3.7

An *R*-module *M* is said to be *free* if it has a basis.   DEF 3.8

3.1 Existence of a Basis

If V is a vector space over $\mathbb{F}$, then V has a basis.

Let $\mathcal{L}$ be the set of all linearly independent sets of V. Inclusion gives a partial   PROOF.
ordering on elements of $\mathcal{L}$. Recall that a partial ordering $\sim$, in addition to
being reflective and symmetric, is such that $x \sim y, y \sim x \implies x = y$. Hence,
$\mathcal{L}$ equipped with inclusion satisfies the maximal chain condition: namely,
if $S \subseteq \mathcal{L}$ is totally ordered under inclusion, then $\exists \Sigma \in \mathcal{L}$ which contains all
elements in S. In particular, one can take $\Sigma = \cup_{B \in S} B$ (we cannot necessarily
take the maximum, as S may be infinite).

Zorn's Lemma states that there is an element $B \in \mathcal{L}$ which is maximal under
inclusion (i.e. if $B \subsetneq B'$, then $B' \notin \mathcal{L}$). We already know that B is linearly
independent. It remains to show that it is spanning. Suppose otherwise, and
let $v \in V$ be s.t. $v \notin \text{span}(B)$. Then $B \cup \{v\}$ is linearly independent, hence
violating maximality of inclusion on $B \implies \notlightning$. Hence, B is a basis. Checking
this last claim a la linear algebra, you'll notice that we need R to be a field.

$\square$

Every $\mathbb{Z}$-module is an abelian group (and vice versa). Every $\mathbb{F}[x]$-module is a   PROP 3.2
vector space over $\mathbb{F}$ equipped with a linear transformation $T : V \to V$ (and vice
versa).

We'll build two-way associations for both. Let M be a $\mathbb{Z}$-module. M is already   PROOF.
an abelian group. Now, let M' be an abelian group. It is a $\mathbb{Z}$-module by
$km' = \underbrace{m' + ... + m'}_{k \text{ times}}$, where $k \in \mathbb{Z}, m' \in N$.

Let V be a vector space over $\mathbb{F}$, and let $T : V \to V$ be a linear transformation.
Then V is an $\mathbb{F}[x]$-module by $f \cdot v = f(T)(v)$, where $f \in \mathbb{F}[x], v \in V$. Now, let
V' be an $\mathbb{F}[x]$-module. Then let $T : V' \to V'$ be $T(v) = x \cdot v$ for $v \in V'$. We
have scalar multiplication by $\lambda v = \lambda v$, where, on the left, $\lambda \in \mathbb{F}$, and on the
right, $\lambda \in \mathbb{F}[x]$. $\square$

♠ *Examples* ♣   E.G. 3.1

1. If $M = \mathbb{R}$ and $R = \mathbb{Q}$, finding a basis is non-trivial (in fact, impossible). Sometimes, this theoretic basis, which only exists as a consequence of the axiom of choice, is called the "Hamel basis."

2. The existence of a basis is far from guaranteed. Take $R = \mathbb{Z}$. Let $M = \mathbb{Z}^n$. A basis for M may be constructed in the standard sense, i.e.

$$\text{Basis} = \{e_1, ..., e_n\} \quad e_i := \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow i^{th} \text{ position}$$

What if $M = \mathbb{Q}$ with $R = \mathbb{Z}$? Then we find that any two elements in M are linearly dependent:

$$\frac{a}{b}, \frac{c}{d} \in M \implies (bc)\frac{a}{b} = ca = ac = \frac{c}{d}(da)$$

So, if an independent set exists, it only has one element. But no single rational spans all of $\mathbb{Q}$, so no basis exists. Even stronger, no finite spanning sets exist on M. Consider a candidate S:

$$S = \left\{ \frac{a_1}{b_1}, ..., \frac{a_N}{b_N} \right\} \implies \frac{1}{a_1 \cdot ... \cdot a_N + 1} \notin \text{span}(S) \implies \lightning$$

What about $M = \mathbb{Z}/n\mathbb{Z}$ with $R = \mathbb{Z}$? We have that $\{1\}$ spans M, but is not linearly independent, since $n \cdot 1 \equiv 0$. Hence, no basis exists for M (recall that the basis is minimally spanning).

PROP 3.3

If $M \subseteq R$ is an R-module, then M is an ideal of R.

PROP 3.4

If $I \triangleleft R$ is an ideal, then I has a basis as an R-module $\iff I = (a) = aR$, i.e. I is principal, where a is not a zero divisor.

MORPHISMS

DEF 3.9

An R-module homomorphism between M_1 and M_2 is a function $f : M_1 \rightarrow M_2$ s.t.

1. f is a group homomorphism from $M_1 \rightarrow M_2$

2. $f(\lambda m) = \lambda f(m) \quad \forall \lambda \in R, m \in M_1$

DEF 3.10

$\ker(f) = \{m \in M : f(m) = 0\}$. Note that, by (2) of the definition above, $\lambda m \in \ker(f)$ if $m \in \ker(f)$. Hence, $\ker(f)$ is an R-submodule of M.

PROP 3.5

If N, M are R-modules with $N \subseteq M$, then M/N is a group and an R-module, where we define $\lambda(m + N) = \lambda m + N$.

PROOF.

M is abelian $\implies$ N is normal. Hence, as groups M/N is a group. For the action $\lambda(m + N) = \lambda m + N$, we have that $\alpha_\lambda : R \to \text{End}(M) : \lambda \mapsto \psi_\lambda$, where $\psi_\lambda(m) = \lambda m$, is a homomorphism. For this new action, we associate $\beta_\lambda : R \to \text{End}(M) : \lambda \mapsto \psi_\lambda + N$. As $\lambda \to \psi_\lambda$ is a homomorphism, $\lambda \to \psi_\lambda + N$ is too. $\qquad\square$

3.2   First Isomorphism Theorem

If $f : M_1 \to M_2$ is a module homomorphism, then it induces an injective homomorphism

$$\overline{f} : M_1/\ker(f) \to M_2 : a + \ker(f) \mapsto f(a)$$

If M is a free R-module with a finite basis, then any two bases of M have the same cardinality.

<div align="right">PROP 3.6</div>

Let I be a proper maximal ideal in R. Consider now the set $IM = \text{span}(\lambda m : \lambda \in I, m \in M)$. Then IM is an R-submodule of M, and so M/IM is an R-module itself, by <u>Prop 3.5</u>. Since I acts as 0 on M/IM, we have that M/IM is a vector space over $\mathbb{F} := R/I$ (which is a field, since I is maximal), where

<div align="right">PROOF.</div>

$$(\lambda + I)(m + IM) = \lambda m + IM$$

If M has a basis of size n, then $M \cong R^n$. Then $M/IM \cong F^n$ as a vector space.

If $\{e_1, ..., e_n\}$ and $\{f_1, ..., f_m\}$ are bases of M, then $M \cong R^n \cong R^m$, so $M/IM \cong F^n \cong F^m$ as a vector space, so $n = m$. $\qquad\square$

If M is a free R-module, then the cardinality of its basis is called the *rank* or *dimension* of M over R.

<div align="right">DEF 3.11</div>

Let $\beta = \{m_1, ..., m_n\}$ be a basis of M. Then we have $R^n \cong M$ by the isomorphism

<div align="right">PROP 3.7</div>

$$\varphi_\beta : R^n \to M : \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix} \mapsto \beta \bullet \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix} = \lambda_1 m_1 + ... + \lambda_n m_n$$

We may conclude that β is a basis $\iff$ φ_β is an R-module isomorphism.

If β', β are two bases for an R-module M, then there is an invertible matrix $P \in \text{GL}_n(R)$ with $\beta' = \beta \cdot P$

<div align="right">PROP 3.8
(Change of basis)</div>

Let $T : M_1 \to M_2$, for free R-modules M_1, M_2 with rank n and m, respectively, be a linear transformation. Let B_1, B_2 be their bases. Then let $M \in M_{m \times n}(R)$ be the matrix whose j^{th} column is given by the coordinates of $T(e_j)$ relative to B_2, where $e_j \in B_1$.

<div align="right">PROP 3.9
AKA: a group homomorphism which also respects $T(\lambda m) = \lambda T(m) \forall \lambda \in R$</div>

Let $\varphi_{B_1} : R^n \to M_1$ and $\varphi_{B_2} : R^m \to M_2$ be the natural transformations taking a vector of constants in R to the corresponding linear combination of vectors in B_1 and B_2, respectively. Then we yield the following commutative diagram:

$$
\begin{array}{ccc}
M_1 & \xrightarrow{\ \ T\ \ } & M_2 \\[2pt]
\varphi_{B_1} \Big\uparrow \wr & & \wr \Big\uparrow \varphi_{B_2} \\[2pt]
R^n & \xrightarrow{\ \ M\ \ } & R^m
\end{array}
$$

EIGENVECTORS

Let $R = \mathbb{F}$ be a field. Let $T : V \to V$ be a linear transformation over a vector space V with basis β. Let $M = [T]_\beta$, and consider the homomorphism

$$
\mathrm{ev}_M : \mathbb{F}[x] \to M_n(\mathbb{F}) : f(x) \mapsto f(M)
$$

ev_M is not injective, since $\dim(M_n(\mathbb{F})) = n^2$ but $\dim(\mathbb{F}[x]) = \infty$. Recall that $\ker(\mathrm{ev}_M)$ is an ideal of $\mathbb{F}[x]$, so it is generated by a unique monic polynomial $p(x)$. We then write $\ker(\mathrm{ev}_M) = \langle p(x) \rangle$.

DEF 3.12 $p(x)$ is called the *minimal polynomial* of M, and we denote it by p_M.

PROP 3.10   For $M \in M_n(\mathbb{F})$, $p_M(M) = 0$, and $f(M) = 0 \implies p_M | f$.

PROOF.

> By definition, $p_M \in \ker(\mathrm{ev}_M)$, so $p_M(M) = 0$. Furthermore, if $f(M) = 0$, then $f \in \ker(\mathrm{ev}_M) = \langle p_M \rangle$, so $f = g p_M$, and hence $p_M | f$. $\hspace{1em}\square$
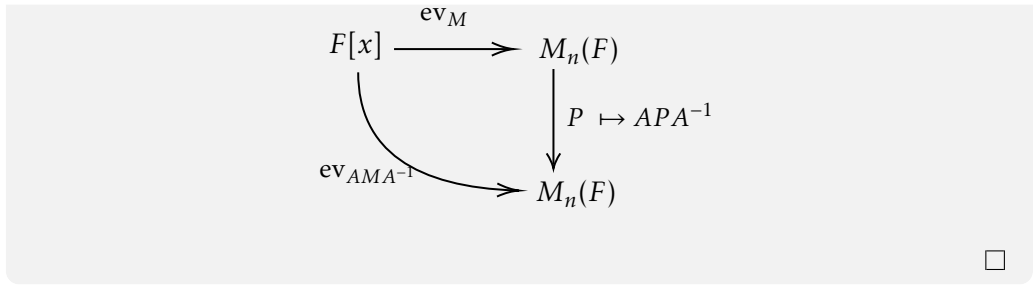
To extend p_M to p_T (i.e. $p_M = p_{M'}$ for any two representations of T), we need to consider alternate bases. (Recall that we fixed $\beta \subseteq V$ in our construction of M.)

PROP 3.11 $p_M = p'_M$ for $M = [T]_\beta$, $M' = [T]_{\beta'}$, and bases $\beta, \beta' \subseteq V$.

PROOF.

> By <u>Prop 3.8</u>, $\beta' = \beta A$ for $A \in \mathrm{GL}_n(\mathbb{F})$. Hence, $M' = AMA^{-1}$, and we need to show $p_M = p_{AMA^{-1}}$. The map $M \mapsto AMA^{-1}$ is an automorphism of $M_n(\mathbb{F})$. Furthermore, we have
>
> $$
> (AMA^{-1})^k = AM^k A^{-1} \quad \text{and} \quad A(M_1 + M_2)A^{-1} = AM_1 A^{-1} + AM_2 A^{-1}
> $$
>
> $f \in \ker(\mathrm{ev}_M) \iff f(M) = 0 \iff Af(M)A^{-1} = 0 \iff f(AMA^{-1}) = 0 \iff f \in \ker(\mathrm{ev}_{AMA^{-1}})$, as viewed by the commutative diagram:

$$\begin{array}{ccc}
F[x] & \xrightarrow{\;\mathrm{ev}_M\;} & M_n(F) \\
& & \Big\downarrow{\scriptstyle P\;\mapsto\;APA^{-1}} \\
& \xrightarrow{\;\;\mathrm{ev}_{AMA^{-1}}\;\;} & M_n(F)
\end{array}$$

$\square$

The *minimal polynomial* of T is the unique monic polynomial over F satisfying   DEF 3.13

$$p(T) = 0 \qquad f(T) = 0 \implies p(x)|f(x)$$

In particular, for $\mathrm{ev}_T : \mathbb{F}[x] \to \mathrm{End}_{\mathbb{F}}(V)$ by $f(x) \mapsto f(T)$, we have $\ker(\mathrm{ev}_T) = \langle p_T \rangle$.

We can think of $\deg(p_T(x))$ as the smallest m such that $\{I, T, T^2, ..., T^{m+1}\}$ certainly is not linearly independent. Let $\dim(V) = n$. Then $\dim(\mathrm{End}(V)) = n^2$, since $\mathrm{End}(V) \cong M_n(F)$. Hence, $\deg p_T(x) \le n^2$.

Note that, if $n > 1$, then $\mathrm{ev}_T : F[x] \to \mathrm{End}(V)$ is *not* surjective. Why? $F[x]$ is commutative, and the image of $F[x]$ under a homomorphism must also be commutative.

Q: What is the largest dimension k of a commutative subring of $\mathrm{End}(V) \cong M_n(F)$? This would bound $\deg p_T(x) \le k \le n^2$.

λ is an eigenvalue of T if $\exists v \in V \setminus \{0\}$ such that $T(v) = \lambda v$ DEF 3.14

3.3 Roots of Minimal Polynomial are Eigenvalues

If $p_T(\lambda) = 0$, then λ is an eigenvalue of T.

$p_T(\lambda) = 0 \implies p_T(x) = (x - \lambda)q(x)$. But also $0 = p_T(T) = (T - \lambda I)q(T)$. We   PROOF. know $q(T) \ne 0$ and $\mathrm{Im}(q(T)) \subseteq \ker(T - \lambda I)$. Hence, if $v \in \mathrm{Im}(q(T))$ for $v \ne 0$, then $(T - \lambda I)(v) = 0 \implies T(v) = \lambda v$. $\square$

3.4 Eigenvalues are Roots of Minimal Polynomial

If λ is an eigenvalue, then $p_T(\lambda) = 0$

We have $T(v) = \lambda v$. Consider any $g(x) \in F[x]$. Then $g(T)(v) = g(\lambda)v$. Fix   PROOF. $v \ne 0$. Then, $0 = p_T(T)(v) = p_T(\lambda)v \implies p_T(\lambda) = 0$. $\square$

3.5 $\deg(p_T(x)) \le n$

PROOF.

If V has a cyclic vector v for T, then we are done. Recall that a cyclic vector v is such that $\{v, ..., T^{n-1}(v)\}$ is linearly independent. This means that $\exists f$ of degree n with $f(T)(v) = 0$. But this means that, in particular, $f(T) = 0$.

Otherwise, we proceed by induction on $\dim(V)$. Consider the following statement: $S_n = $ "If T is an homomorphism of a vector space V of dimension n, then $\deg(p_T(x)) \leq n$."

Let $v \neq 0 \in V$. Consider $W = \text{span}(v, T(v), ..., T^k(v), ...)$. Assume that $W \neq V$, or else we'll have that v is a cyclic vector. Note that W is then stable under T (i.e. maps to itself under T).

If W is T-stable, then T induces a homomorphism

$$\overline{T} : V/W \rightarrow V/W \quad v + W \mapsto T(v) + W$$

which is well-defined. As proof, suppose $v_1 + W = v_2 + W$. Then $v_1 - v_2 \in W$, so, since W is T-stable, $T(v_1 - v_2) \in W$. Hence $T(v_1) - T(v_2) \in W$, so $T(v_1) + W = T(v_2) + W$.

Consider now $p_{\overline{T}}(x)$ and p_{T_W}. By induction hypothesis, we know that $\deg(p_{\overline{T}}) \leq \dim(W)$ and $\deg(p_{T_W}) \leq \dim(V/W)$.

We claim that $p_{T_W}(x)p_{\overline{T}}(x)$ vanishes on T. By definition, we know $p_{\overline{T}}(\overline{T}) = 0$. Hence, $p_{\overline{T}}(\overline{T})(v + W) = 0$, i.e. $p_{\overline{T}}(T)(v) + W = 0$, so $p_{\overline{T}}(T)(v) \in W$. $\square$

PROOF.

We could, at first, note that $p_T | f_T$, where $f_T = \det(\lambda I - t)$ is the characteristic polynomial, which has degree $\leq n$. But we haven't yet seen these.

Recall from homework: let T be of order 7 in $\text{GL}_3(F_2) \cong \text{End}_{F_2}(F_2^3)$. Let $f = x^7 - 1$.

1. $p_T(1) \neq 0$. Otherwise, T has an eigenvalue, so $\exists v : Tv = v$. But then $T \in \text{stab}(v)$, which has cardinality $\frac{168}{7} = 24$. But T has order 7, which doesn't divide 24.

2. For $v \neq 0$, $\{v, T(v), T^2(v)\}$ are linearly independent, and hence a basis for V. Write $a_0 v + a_1 T(v) + a_2 T^2(v) = 0$. Then, rewriting $f(x) = a_0 + a_1 T + a_2 T^2$, we have $f(T)(v) = 0$. So, in particular, $f(T)$ has non-trivial kernel, and is not invertible. But $\gcd(f(x), p_T(x)) = 1$.

   Lemma: If $\gcd(f(x), p_T(x)) = 1$, then $f(T)$ is invertible. Let $1 = a(x)f(x) + b(x)p_T(x)$. Evaluating at T, we have $I = a(T)f(T) + b(T)p_T(T) \implies I = a(T)f(T)$, so $a(T) = f^{-1}(T)$. (Note: this gives an algorithm for finding an inverse of a function, in terms of the Euclidean algorithm, given that the minimal polynomial is known!)

Hence, $T^3(v)$ is a linear combination of $v, T(v), T^2(v)$. Hence, $\exists f = a_0 + a_1 x + a_2 x^2 + a_3 x^3$ such that $f(T)(v) = 0$. But, in particular, $T \circ f(T)(v), T \circ f(T)(T(v))$, and $T \circ f(T)(T^2(v)) = 0$, so $f(T) = 0$.

$\square$

Quotients

If $N \subseteq M$ are R-modules, then M/N is also an R-module.

If M, N are *free* over R, then M/N need not be free.

──────────────────── ♠ *Examples* ♣ ────────────────────

1.

2. $M = \mathbb{Q}, N = \mathbb{Z}, R = \mathbb{Z}$. M is not free. And M/N is not free either (any singleton a is not linearly independent, by multiplying by the denominator).

3. $M = \mathbb{Z}, N = m\mathbb{Z}, M/N = \mathbb{Z}/m\mathbb{Z}$. Both $\mathbb{Z}$ and $m\mathbb{Z}$ are free, but M/N is not.

──

If $R = \mathbb{F}$ is a field and $W \subseteq V$ are F-vector spaces, then V/W is a vector space.

3.6   Something
$$\dim(V) = \dim(W) + \dim(V/W)$$

$m = \dim(W), n = \dim(V)$. Let $(v_1, ..., v_m)$ be a basis for W. We can complete it to a basis $(v_1, ..., v_m, v_{m+1}, ..., v_n)$ for V. We then claim that $v_{m+1} + W, ..., v_n + W$ form a basis for V/W.

Let $v + W \in V/W$. We can write $v = \lambda_1 v_1, ..., \lambda_n v_n$. But then $v + W = \lambda_{m+1}(v_{m+1} + W) + ... + \lambda_n(v_n + W)$.

For linearly independence, suppose $\exists \lambda_1, ..., \lambda \in \mathbb{F}$ such that

$$\lambda_{m+1}(v_{m+1} + W) + ... + \lambda_n(v_n + W) = 0$$

we can re-write this as

$$(\lambda_{m+1} v_{m+1} + ... + \lambda_n v_n) + W = 0$$

Thus, $\exists \lambda_1, ..., \lambda_m$ such that

$$\lambda_{m+1} v_{m+1} + ... + \lambda_n v_n = -\lambda_1 v_1 - ... - \lambda_m v_m$$

But we have linear independence of $v_1, ..., v_n$, so in particular $\lambda_1, ..., \lambda_n = 0$.

$\square$

PROP 3.12

If $T : V \to V$ is a linear transformation, and W is a T-stable subspace, then T induces

$$\overline{T} : V/W \to V/W \quad v + W \mapsto T(v) + W$$

Importantly, it is not always true that W has a T-stable complement.

E.G. 3.3

─────────────────────── ♠ *Examples* ♣ ───────────────────────

1. Consider $T : V \to W$ to be the projection of V onto W. Then $T^2 = T$, and indeed W is T-stable. Notice that $\ker(T)$ is a complimentary subspace of W. In particular, $v = Tv + (v - Tv) = Tv + u$ with $u \in \ker(T)$, since $T(v - Tv) = Tv - T^2v = Tv - Tv = 0$.

2. $V = \mathbb{F}_2^2$. Let $T\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$ and $T\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}$. Let $W = F\begin{pmatrix}1\\0\end{pmatrix}$. This is T-stable by definition. Let $W' = F\begin{pmatrix}\lambda\\1\end{pmatrix}$ (which is complimentary to W). Then $T\begin{pmatrix}\lambda\\1\end{pmatrix} = \begin{pmatrix}\lambda + 1\\1\end{pmatrix}$, so W is *not* T-stable.

───

How can we understand $T : V \to V$. First, find a non-trivial T-stable $W \subseteq V$ and a non-trivial T-stable $W' \subseteq V$ which is complimentary to V. Then

$$V = W \oplus W'$$

PROP 3.13

$p_T(x)$ divides $p_{T|_W} \circ p_{\overline{T}}$.

PROOF.

We know that $p_{\overline{T}}(T)$ maps V to W, and $p_{T|_W}$ maps W to 0. hence $p_{T|_W} \circ p_{\overline{T}}(T) = 0$, so p_T divides it. $\square$

Proof of 3.6 (continued)

PROOF.

We proceed by induction on $\dim(V)$. Choose $v \neq 0$. Consider $W = \text{span}(v, T(v), ..., T^k(v))$. *Case 1*: $W = V$. Then W is T-stable. *Case 2:* $W \subseteq V$. Then p_T divides $p_{T|_W} p_{\overline{T}}$, so in particular $\deg(p_T) \leq \deg(p_{T|_W}) + \deg(p_{\overline{T}}) \leq \dim(W) + \dim(V/W) = \dim(V)$ by induction hypothesis. $\square$

Primary Decomposition Theorems

Consider V and $T : V \to V$. Then T endows V with the structure of an $\mathbb{F}[x]$ module, where the action of $\mathbb{F}[x]$ on V is given by $f(x) \cdot v = f(T)(v)$. Conversely, an $\mathbb{F}[x]$ action on V can generate $T(v) = xv$.

Just as $\mathbb{F}[x]$ modules are somewhat the same as vector spaces V equipped with a transformation T, $\mathbb{Z}$ modules are somewhat the same as abelian groups.

> **3.7   Primary Decomposition Theorem**
>
> Suppose that $p_T(x)$ factors into $p_1(x)p_2(x)$ with $\gcd(p_1, p_2) = 1$. Then there exists unique subspaces $V_1, V_2 \subseteq F$ such that
>
> 1. $V = V_1 \oplus V_2$
>
> 2. V_j is stable under T
>
> 3. The minimal polynomial of $T_j := T|_{V_j}$ is $p_j(x)$

Concretely, we have $V_1 = \ker(p_1(T))$ and $V_2 = \ker(p_2(T))$.

For example, consider an idempotent transformation $T^2 = T$. Then $p_T(x) = x^2 - x = x(x - 1)$. Then $p_1 = x$ and $p_2 = x - 1$. Then, the theorem above says that $V = V_1 \oplus V_2$, and we conclude that $V_1 = \ker(T)$ and $V_2 = \text{Im}(T)$.

$\mathbb{F}[x]/\langle p_T(x) \rangle \cong \mathbb{F}[x]/\langle p_1(x) \rangle \times \mathbb{F}[x]/\langle p_2(x) \rangle.$

<div style="text-align:right">PROP 3.14
Chinese Remainder Theorem</div>

> Consider the homomorphism $\mathbb{F}[x]/\langle p_T(x) \rangle \to \mathbb{F}[x]/\langle p_1(x) \rangle \times \mathbb{F}[x]/\langle p_2(x) \rangle$ by $f(x) \to (f(x) + \langle p_1(x) \rangle, f(x) + \langle p_2(x) \rangle)$. The kernel of this homomorphism is exactly $\{f(x) : p_1(x)|f(x) \text{ and } p_2(x)|f(x)\} = \{f(x) : p_T(x)|f(x)\} = \langle p_T(x) \rangle$, which is 0 in the domain.
>
> PROOF.
>
> For surjectivity, we compute the dimensions of both sides (as vector spaces). Consider $\dim(\mathbb{F}[x]/\langle p_T(x) \rangle)$. We may write
>
> $$\mathbb{F}[x]/\langle p_T(x) \rangle = \{a_0 + \ldots + a_m x^m + \langle p_T(x) \rangle \quad m = \deg(p_T(x)) - 1\}$$
>
> Hence, a basis is $\{1, \ldots, x^m\}$, which has size $m + 1 = \deg(p_T(x))$.
>
> Then, by the same arguments, we have that $\dim(\mathbb{F}[x]/\langle p_1(x) \rangle) = \deg(p_1(x))$ and $\dim(\mathbb{F}[x]/\langle p_2(x) \rangle) = \deg(p_2(x))$, and lastly $\deg(p_T) = \deg(p_1) + \deg(p_2) = \dim(\mathbb{F}[x]/\langle p_1(x) \rangle \times \mathbb{F}[x]/\langle p_2(x) \rangle)$. $\qquad\square$

If M_1 is a module over R_1, and M_2 is a module over R_2, then $M_1 \times M_2$ is an $(R_1 \times R_2)$ module, where, for $(\lambda_1, \lambda_2) \in R_1 \times R_2$ and $(m_1, m_2) \in M_1 \times M_2$, $(\lambda_1, \lambda_2)(m_1, m_2) = (\lambda_1 m_1, \lambda_2 m_2)$.

<div style="text-align:right">PROP 3.15</div>

3.8 Module Decomposition

If M is a module over $R_1 \times R_2$, then there are R_i modules, M_i, for $i = 1, 2$, such that

$$M \cong M_1 \times M_2$$

PROOF.

We can conceptualize R_1 as an ideal of $R_1 \times R_2$, by $\{(a, 0) : a \in R_1\}$. Similarly for R_2. Define now $M_1 = (1, 0)M$ and $M_2 = (0, 1)M$.

Consider $m \in M$. This is $(1, 1)m$, since m is over $R_1 \times R_2$. But this is $(1, 0)m + (0, 1)m$. Then $(1, 0)m \in M_1$ and $(0, 1)m = M_2$. We also need to show that $M_1 \cap M_2$ is trivial. If there exists m with $m = (1, 0)m_1 = (0, 1)m_2$, then by multiplying by $(1, 0)$, we get $(1, 0)m_1 = (0, 0)m_2 = 0$, so indeed $m = 0$. □

As a corolllary, we get <u>Thm 3.8</u>.

PROOF.

V is a module over $\mathbb{F}[x]/\langle p_T(x)\rangle = \mathbb{F}[x]/p_1(x) \times \mathbb{F}[x]/p_2(x)$, so V decomposes into $V_1 \oplus V_2$, where V_1 is an $\mathbb{F}[x]/p_1(x)$ module, and V_2 is an $\mathbb{F}[x]/p_2(x)$ module.

Let $V_1 = \ker(p_1(T))$ and $V_2 = \ker(p_2(T))$.

Since $\gcd(p_1, p_2) = 0$, we can write $1 = a(x)p_1(x) + b(x)p_2(x)$. Hence, evaluating at T, we get $T = a(T)p_1(T) + b(T)p_2(T)$. Then, $\forall v \in V$, we can write $v = \underbrace{a(T)p_1(T)(v)}_{\in V_2} + \underbrace{b(T)p_2(T)(v)}_{\in V_1}$.

We also observe that $V_1 \cap V_2 = \{0\}$, since, if $v \in V_1, V_2$, then $v = 0 + 0 = 0$ from above. □

3.9 PDT 2

If $p_T = p_1^{e_1} \cdot \ldots \cdot p_t^{e_t}$, where $p_1, \ldots, p_t$ are irreducible, then

$$V = V_1 \oplus \ldots \oplus V_t$$

where $p_{T|_{V_i}} = p_i(x)^{e_i}$.

PROOF.

We can show by induction on t, utilizing <u>Thm 3.9</u> from above. □

DEF 3.15

Given $T : V \to V$ and $\lambda \in \mathbb{F}$, the *eigenspace* of T corresponding to λ is

$$V_\lambda = \text{Eig}_T(\lambda) = \{v \in V : T(v) = \lambda v\} = \ker(T - \lambda)$$

Similarly, the *generalized eigenspace* corresponding to λ is

$$V_{(\lambda)} = \{v \in V : \exists m \geq 1 : (T - \lambda)^m(v) = 0\} = \cup_{m \geq 1} \ker\left((T - \lambda)^m\right) = \ker\left((T - \lambda)^e\right)$$

3.10   PDT 3

Suppose that F is algebraically closed, i.e. $p_T(x) = (x - \lambda_1)^{e_1} \cdot \ldots \cdot (x - \lambda_t)^{e_t}$. Then V decomposes into generalized eigenspaces, i.e.

$$V = V_1 \oplus \ldots \oplus V_t$$

where $T|_{V_i}$ has minimal polynomial $(x - \lambda_i)^{e_i}$. In particular

$$V_j = \ker\left((T - \lambda_j)^{e_j}\right)$$

If $e_1, \ldots, e_t = 1$, then V_i will just act as multiplication. Hence V_i will be the eigenspace for λ_i, and T will be diagonalizable.

There is a basis for $V_{(\lambda)}$ for which the matrix of T is of the form

$$[T] = \begin{pmatrix} J_{1,\lambda} & 0 & \cdots & 0 \\ 0 & J_{2,\lambda} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_{m,\lambda} \end{pmatrix} \quad \text{where} \quad J_{1,\lambda} = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ 0 & 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}$$

This is the *Jordan canonical form*.

MODULES OVER PIDS

A module M over a ring R is called *finitely generated* if it has a finite spanning
set.

3.11   Structure Theorem

Let M be an finitely generated module over a principal ideal domain R. Then $\exists d_1 | d_2 | \cdots | d_t$ and an integer $m \geq 0$ such that

$$M \cong R/(d_1) \oplus \cdots \oplus R/(d_t) \oplus R^m$$

Then, $d_1, \ldots, d_t$ are called the *elementary divisors* of M, and m is called the *rank* of M over R.

Note that M is free $\iff t = 0$.

──────────────────────────── ♠ *Examples* ♣ ────────────────────────────

1. If G is a finitely generated abelian group, then

$$G = \mathbb{Z}/(n_1) \oplus \cdots \oplus \mathbb{Z}/(n_t) \oplus \mathbb{Z}^m$$

   and G is finite if $m = 0$.

2. If V is a generalized eigenspace for T corresponding to λ, then

$$V = \mathbb{F}[x]/(x - \lambda)^{n_1} \oplus \cdots \oplus F[x]/(x - \lambda)^{n_i} \oplus F[x]^m$$

   where $n_1 \leq n_2 \leq ... \leq n_t$.

3.12   Lemma

If M is a finitely generated R-module, then it is a quotient of a free R module.

PROOF.

Let $m_1, ..., m_t$ be a set of R module generators for M. Then consider $\varphi : R^t \to M$ by $(\lambda_1, ..., \lambda_t) \to \lambda_1 m_1 + ... + \lambda_t m_t$. This is a surjective homomorphism, since M is finitely generated. Hence, $M \cong R^t / \ker(\varphi)$. $\qquad \square$

Q: Show that $\mathbb{Q}$ is not the quotient of a free $\mathbb{Z}$ module.

DEF 3.19

An R-module is *cyclic* if it is isomorphic to R/I for some ideal $I \triangleleft R$. Equivalently, M is cyclic if it can be generated by one element. Note that $(1 + I)$ generates R/I as an R-module, so M is hence generated by 1 element.

PROOF OF STRUCTURE THEOREM

Express M as a quotient R^n/N, where N is as in <u>Thm 3.13</u>.

Claim: If N is an R-submodule of a free R-module of rank n, then N is also free or rank $\leq n$.

Proof: By induction on n. If $n = 1$, with $N \subseteq R$, the R-submodule N is an ideal of R. Hence $\exists a \in R$ s.t. $N = aR$. We form the isomorphism $N \to R : \lambda \mapsto \lambda a$. This is clearly surjective. Since $a \neq 0$, and a is not a zero divisor, this is also injective.

Now suppose $N \subseteq R^{n+1}$. Consider the R-module homomorphism $\varphi : R^{n+1} \to R$ which sends $(\lambda_1, ..., \lambda_{n+1}) \to \lambda_{n+1}$. Then $\varphi(N)$ is an ideal of R, so we may write $\varphi(N) = aR$. Choose $m_{n+1} \in N$ s.t. $\varphi(m_{n+1}) = a$. Consider $N \cap \ker(\varphi)$, where, in particular

$$\ker(\varphi) = \{(\lambda_1, ..., \lambda_n, 0) : \lambda_i \in R\} \cong R^n$$

Case 1: $a = 0$, then $\varphi(N) = 0$, so $N \subseteq \ker(\varphi) = R^n$. In particular, then, N is free of rank $\leq n$.

Case 2: $a \neq 0$, then by induction hypothesis $N \cap \ker(\varphi)$ is free of rank $\leq n$. On the other hand, $N \cong (N \cap \ker(\varphi)) \oplus R$. To show this, consider the mapping

$$\eta : (n_0, \lambda) \longmapsto n_0 + \lambda m_{n+1}$$

For surjectivity: given $n \in N$, we claim $\exists \lambda \in R$ with $n - \lambda m_{n+1} \in \ker(\varphi)$. Indeed, $\varphi(n) - \lambda \varphi(m_{n+1}) = 0 \implies \varphi(n) = \lambda a \implies \lambda = \frac{\varphi(n)}{a}$.

Hence, $n_0 := n - \lambda m_{n+1} \in N \cap \ker(\varphi)$, and so $n = n_0 + \lambda m_{n+1} = \eta(n_0, \lambda)$, so η is surjective.

For injectivity: $\eta(n_0, \lambda) = 0 \implies n_0 + \lambda m_{n+1} = 0 \implies \varphi(n_0 + \lambda m_{n+1}) = 0 \implies \lambda \varphi(m_{n+1}) = 0 \implies \lambda a = 0 \implies \lambda = 0$.

Thus, $N \cong N_0 \oplus R$, where $N_0 \subseteq R^n$ is free of rank $\leq n$. We can write then $N_0 \cong R^m$ for $m \leq n$. Hence $N \cong R^{m+1}$ with $m + 1 \leq n + 1$.

Thus, if M is a finitely generated R-module, then $M \cong \mathbb{R}^n / N$, where $N \cong R^m$ and $m \leq n$. Let $v_1, ..., v_m$ be a basis for N, where we adopt the conventionn

$$v_i = \begin{bmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{bmatrix} \quad v_{m+i} = 0 \; \forall i$$

Then, we let $A = [v_1, ..., v_n]$, and have $R^m = AR^n$, and so $M = R^n / AR^n$.

Note, if $Q^{-1} \in \mathrm{GL}_n(R)$, then $R^n / (AQ^{-1}R^n) = R^n / AR^n$ (since $Q^{-1}R^n = R^n$ up to a change of basis). Similarly, we claim that R^n / PAR^n, where $P \in \mathrm{GL}_n(R)$. To show this, we have $PR^n / PAR^n \cong R^n / AR^n$ by $Pv \leftrightarrow v$, but then $PR^n = R^n$ as before.

Consider the group action $\mathrm{GL}_n(R) \times \mathrm{GL}_n(R)$ on $M_n(R)$ by $(P, Q)(A) = PAQ^{-1}$. For any $A \in M_n(R)$, the orbit of A under this action contains a matrix of the form

$$\begin{bmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & \ddots & \\ 0 & & & d_n \end{bmatrix}$$

$\square$

where $d_1 | d_2 | \dots | d_n$ (some may be 0). Recall that AQ for $Q \in GL_n(R)$ corresponds to column operations, and PA row operations.

> **3.13**
>
> Let $M = R^n$ and let $N \subseteq M$ be a free R-module. Then there exists a basis for M, $\{m_1, ..., m_n\}$ such that N is spanned by $\{d_1 m_1, ..., d_n m_n\}$ with $d_1 | d_2 \cdots | d_n$.
>
> Note: it may be that $d_t, ..., d_n$ are 0 for some $t \geq 1$. If they are all non-zero, then $\{d_1 m_1, ..., d_n m_n\}$ are linearly independent.

PROOF.

If this holds, then remark: if $v = \lambda_1 m_1 + ... + \lambda_n m_n \in M$, then $v \in N \iff d_1 | \lambda_1, ..., d_n | \lambda_n$. Hence, $M/N = M/AM$, where A has d_i in the diagonals. But this is the same as $(R/d_1 R) \times \cdots \times (R/d_n R)$.

We'll show by induction on n. If $n = 1$, then $M = R$ and $N \subseteq R$. We may let $m_1 = 1$ be a basis for M. Then, N is an ideal, and since R is a PID, this means $N = d_1 R$ for some d_1. Hence, n is spanned by $d_1 m_1$.

For $n \to n+1$, let $M = R^{n+1}$. We'll want to choose $n_1 \in N$ which is as "little divisible as possible," i.e.

Given $\varphi \in \operatorname{Hom}(M, R)$, i.e. a homomorphism from $M \to R$. Let $\varphi(N) = \operatorname{Im}(\varphi|_N)$, i.e. the image of φ on N. Then $\varphi(N) \subseteq R$ is an R-submodule of R, hence an ideal of R. We can then write $I(\varphi) = \langle d \rangle$. Let

$$\Sigma = \{\varphi(N) : \varphi \in \operatorname{Hom}(M, R)\}$$

Σ is partially ordered by inclusion. Let $\langle d_1 \rangle = \varphi_1(N)$ be a maximal element of Σ (it satisfies the maximal chain property, since R is a PID). $\exists n_1 \in N$ s.t. $\varphi_1(n_1) = d_1$.

We claim that n_1 is divisible by d_1. As proof, let $\eta_1, ..., \eta_n$ be the natural projections $M = R^n \to \mathbb{R}$ which send

$$\eta_j \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_{n+1} \end{pmatrix} = \lambda_j$$

Thus, if $n_1 = \langle x_1, ..., x_{n+1} \rangle$, we need to show $d_1 | x_j = \eta_j(n_1) \; \forall j$. Let $d = \eta_j(n_1)$ and $d_0 = \gcd(d_1, d)$. We can write $d_0 = r d_1 + s d$ for $r, s \in R$. Rewriting, we have $d_0 = r \varphi_1(n_1) + s \eta_j(n_1) = (r \varphi_1 + s \eta_j)(n_1)$. Then $r \varphi_1 + s \eta_j \in \operatorname{Hom}(M, R)$, so $\langle d_0 \rangle \in \Sigma$ and $d_0 | d_1$. By maximality of $\langle d_1 \rangle$, $d_1 | d_0$, so $\langle d_0 \rangle = \langle d_1 \rangle$. But $d_0 | d$, and hence $d_1 | d$. So n_1 is divisible by d_1.

Hence, consider $d_1 m_1 = n_1$ as above. Then $\varphi_1(d_1 m_1) = \varphi_1(n_1) = d_1$. Since φ_1 is R-linear, we can write $d_1 \varphi(m_1) = d_1 \implies \varphi(m_1) = 1$.

We now map bijectively $M \to Rm_1 \oplus \ker(\varphi_1)$ by $m \mapsto (\varphi_1(m)m_1, m - \varphi_1(m)m_1)$. One may check that the second coordinate is indeed in $\ker(\varphi_1)$.

Similarly, for $N \subseteq M$, we write $N = Rn_1 \oplus (\ker(\varphi_1) \cap N)$. Denote $M_2 = \ker(\varphi_1)$ and $N_2 = \ker(\varphi_1) \cap N$. Since $N_2 \subseteq M_2$, by induction hypothesis $\exists m_2, ..., m_{n+1}$ which is a basis for M_2, where also $\exists d_2, ..., d_{n+1}$ are s.t. $d_i | d_{i+1}$ and $\{d_2 m_2, ..., d_{n+1} m_{n+1}\}$ spans N_2. Then:

1. $m_1, ..., m_{n+1}$ is a basis for M.

2. $d_1 m_1, ..., d_{n+1} m_{n+1}$ spans N.

it only remains to show that $d_1 | d_2$. For the proof of this, denote $d_i m_i = n_i$.

Let η_j be the jth coordinate homomorphism relative to the basis $(m_1, ..., m_{n+1})$, i.e. if $m = \lambda_1 m_1 + ... + \lambda_{n+1} m_{n+1} \implies \eta_j(m) = \lambda_j$. Observe then

$$\eta_1(n_1) = d_1 \qquad \eta_2(n_1) = 0 \qquad \eta_1(n_2) = 0 \qquad \eta_2(n_2) = d_2$$

Let $d_0 = \gcd(d_1, d_2) = rd_1 + sd_2 : r, s \in R$. We can write $\eta = r\eta_1 + s\eta_2 \in \text{Hom}(M, R)$. Then $\eta(n_1 + n_2) = r\eta_1(n_1) + r\eta_1(n_2) + s\eta_2(n_1) + r\eta_2(n_2) = rd_1 + sd_2 = d_0$. By maximality of d_1, we have $d_1 | d_0$. But $d_0 | d_2$, so $d_1 | d_2$. $\qquad\square$

Hence, we can write $M/N = R^n / (d_1 R \oplus \cdots \oplus d_n R)$, so in particular $M/N = (R/d_1 R) \oplus \cdots \oplus (R/d_n R)$.

───────────────────────── ♠ *Examples* ♣ ─────────────────────────   E.G. 3.5

1. What if $R = \mathbb{Z}$? Then

$$A = \mathbb{Z}/d_1 \oplus \cdots \oplus Z/d_t \oplus \mathbb{Z}^n$$

   A is then an abelian group. A is finite $\iff n = 0$. How can we interpret $d_1, ..., d_t$? Given $a \in A$, $d_t a = 0$, since $(d_t a_1, ..., d_t a_t) = (0, ..., 0)$ (recall $d_i | d_t$). In particular, $d_t = \min\{d \in \mathbb{Z} : da = 0 \forall a \in A\}$. This is called the "exponent" of A.

   $d_1 \cdots d_t$ will be the order of A.

   Note that, for finite abelian groups, having the same order and exponent does not imply isomorphism. As an example, consider

$$A_1 = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \qquad A_2 = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$

2. What if $R = \mathbb{F}[x]$. Then

$$M = \mathbb{F}[x]/d_1(x) \oplus \cdots \oplus \mathbb{F}[x]/d_t(x) \oplus \mathbb{F}[x]$$

where $d_i(x) \in \mathbb{F}[x]$ are polynomials. We can view M not only as a module over $\mathbb{F}[x]$, but a vector space over $\mathbb{F}$, and hence $r = 0 \iff \dim(M) < \infty$. Furthermore, we can then write $\dim(M) = \dim(\mathbb{F}[x]/d_1(x)) + \ldots + \dim(\mathbb{F}[x]/d_t(x)) = \deg(d_1) + \ldots + \deg(d_t)$.

$\mathbb{F}[x]$ modules with $r = 0$ are exactly (V, T) pairs for finite dimensional vector spaces V and a linear transformation $T : V \to V$. To transform (V, T) to an $\mathbb{F}[x]$-module, we let $f \cdot v = f(T)(v)$. Conversely, given an $\mathbb{F}[x]$-module V, we create $T(v)$ by writing $T(v) = x \cdot v$.

d_t is the minimal degree polynomial such that $d \cdot v = 0 \forall v \in V$, i.e. the minimal polynomial of T, since $d \cdot v = d(T)(v)$.

PROP 3.16

For a finite dimensional vector space V endowed with $T : V \to V$, with structural representation $\mathbb{F}[x]/d_1(x) \oplus \cdots \oplus \mathbb{F}[x]/d_t(x)$, the product $d_1 \cdot \ldots \cdot d_t$ is the characteristic polynomial of T.

PROOF.

Observe the following facts about the characteristic polynomial f_T of T:

1. $p_T | f_T$

2. $\deg(f_T) = \dim(V)$

3. If $V = V_1 \oplus V_2$ as an $\mathbb{F}[x]$-module, then $f_T = f_{T|_{V_1}} f_{T|_{V_2}}$

This last point requires some justification. Choose a basis $(v_1, \ldots, v_m)$ for V_1 and $(v_{m+1}, \ldots, v_n)$ for V_2. Then we will be able to write

$$[T] = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

for block matrices A_1 and A_2 corresponding to the bases for V_1 and V_2, respectively. Then

$$f_T = \det\left(xI - \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}\right) = \det\begin{pmatrix} xI_m - A_1 & 0 \\ 0 & xI_{n-m} - A_2 \end{pmatrix}$$

Consider again the main proposition: if $t = 1$, then $V = \mathbb{F}[x]/p(x)$, then $\deg(p_T) = n$, so in particular $p_T = f_T$.

Generally, if $V = \mathbb{F}[x]/p_1 \oplus \cdots \oplus \mathbb{F}[x]/p_t = V_1 \oplus \cdots \oplus V_t$, we have, by point (3) above,

$$f_T = f_{T|_{V_1}} \cdot \ldots \cdot f_{T|_{V_t}} = p_1 \cdot \ldots \cdot p_t$$

$\square$

Putting these previous examples together...

	$\mathbb{Z}$	$\mathbb{F}[x]$
Finitely generated modules	F.G. abelian groups	F.G.
$\mathbb{F}[x]$-modules $r = 0$	finite abelian groups	finite-dimensional V with $T : V \to V$
d_t	exponent	minimal polynomial
$d_1 \cdot ... \cdot d_t$	cardinality	characteristic polynomial

Recall that, if $M_1, M_2 \in M_n(\mathbb{F})$ are conjugate, then $p_{M_1} = p_{M_2}$ and $f_{M_1} = f_{M_2}$. What about the converse?

M_1 and $M_2 \in M_n(\mathbb{F})$ are conjugate if and only if they have the same elementary divisors (in their structural decomposition).

<div style="text-align: right">PROP 3.17</div>

> Let $V = \mathbb{F}^n$. Let $M_1, M_2 : V \to V$. V can be viewed as an $\mathbb{F}[x]$ module in two different ways: let V_1 and V_2 be V equipped with M_1 and M_2, respectively. In particular, in V_1, $fv = f(M_1)(v)$, and in V_2, $fv = f(M_2)(v)$.
>
> Suppose that V_1 and V_2 have the same elementary divisors $d_1, ..., d_t$. Then $V_1 \cong \mathbb{F}[x]/d_1 \oplus ... \oplus \mathbb{F}[x]/d_t \cong V_2$ as $\mathbb{F}[x]$-modules. Hence, $j : V_1 \to V_2$ is an isomorphism as $\mathbb{F}[x]$-modules, preserving $j(xv) = xj(v)$, i.e. $j(M_1 v) = M_2 j(v)$. Hence $jM_1 = M_2 j$. In particular, j is a transformation itself, so $M_2 = jM_1 j^{-1}$. $\qquad\square$

<div style="text-align: right">PROOF.</div>

––––––––––––––––––– ♠ *Examples* ♣ –––––––––––––––––––

<div style="text-align: right">E.G. 3.6</div>

Let $G = \mathrm{GL}_3(\mathbb{F}_2)$, where $\#G = 168$. The conjugacy classes in G are in bijection with possible sequences $d_1, ..., d_t$ of elementary divisors.

If $t = 1$, then $d_1(x)$ is a polynomial of degree 3 in $\mathbb{F}_2$. Since $A \in \mathrm{GL}_3(\mathbb{F}_2)$ are invertible, $d_1(x)$ cannot be divisible by x. We write:

$$d_1 = x^3 + (?)x^2 + (?)x + 1$$

(a) $d_1 = x^3 + 1 = (x + 1)(x^2 + x + 1)$. Writing $V = V_1 \oplus V_2$, where V_1 is 1-dim and V_2 is 2-dim, we have $T_2^2 = T + 1$ and $T_2^3 = 1$, where T_2 is T restricted to V_2. Hence, the corresponding conjugacy classes are order 3 matrices.

(b) $d_1 = x^3 + x + 1$ 7A

(c) $d_1 = x^3 + x^2 + 1$ 7B

(d) $d_1 = x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1) = (x + 1)^3$. Then $T^3 = T^2 + T \implies T^4 = T^3 + T^2 + T = 2(T^2 + T) + 1 = 1$, so we get a conjugacy class of order 4 elements (4A).

If $t = 2$, then $(d_1, d_2) = (x + 1, (x + 1)^2)$ only. (The first coordinate cannot be x, the second cannot be degree 3 (why?)).

$F_2^3 = \mathbb{F}_2[x]/(x + 1) \oplus \mathbb{F}[x]/(x + 1)^2 = \mathbb{F} \oplus \mathbb{F}[\varepsilon]/\varepsilon^2$, where $\varepsilon = x + 1$.

Then $A \leftrightarrow (1, 1 + \varepsilon)$ and $A^2 \leftrightarrow (1, 1 + 2\varepsilon + \varepsilon^2) = (1, 1) = I$, so order 2 matrices (2A).

If $t = 3$, then $(d_1, d_2, d_3) = (x + 1, x + 1, x + 1)$, but this just corresponds to the identity element (1A).

Now can we compute # of $1A, 2A, 3A, 4A, 7A, 7B$?

3.14 Centralizers in $GL_3(\mathbb{F}_2)$

If $t = 1$, then $Z_G(A) = (\mathbb{F}[x]/d_1)^\times$.

PROOF.

We write $V \cong \mathbb{F}[x]/d_1$ as an $\mathbb{F}[x]$-module. Then $Z_G(A)$ is $\mathrm{Aut}(V) = \mathrm{Aut}(\mathbb{F}[x]/d_1)$ as $\mathbb{F}[x]$-modules. Note that, $B \in Z_G(A) \iff BA = AB \iff BA(v) = AB(v) \forall v \in V$, so in particular $B(xv) = xB(v)$. This means that B is an automorphism which preserves the $\mathbb{F}[x]$ action.

Lastly, we have $\mathrm{Aut}(\mathbb{F}[x]/d_1) = (\mathbb{F}[x]/d_1)^\times$, as desired. $\square$

E.G. 3.7

♠ *Examples* ♣

$Z_G(3A) = (\mathbb{F}[x]/(x^3 + 1))^\times = (\mathbb{F}_2 \times \mathbb{F}_2[x]/(x^2 + x + 1))^\times$, which is exactly $(\mathbb{F}_2 \times \mathbb{F}_4)^\times = \mathbb{F}_2^\times \times \mathbb{F}_4^\times = 1 \times (\mathbb{Z}/3\mathbb{Z})$.

$Z_G(7A) = (\mathbb{F}_2[x]/(x^3 + x + 1))^\times = (\mathbb{F}_8)^\times = \mathbb{Z}/7\mathbb{Z}$ (similarly for $7B$).

$Z_G(4A) = (\mathbb{F}_2[x]/(x + 1)^3)^\times = (\mathbb{F}_2[\varepsilon]/(\varepsilon^3))^\times = \{a + b\varepsilon + c\varepsilon^2 : a, b, c \in \mathbb{F}_2\}^\times$. Then we have $\{1 + b\varepsilon + c\varepsilon^2\}$. Hence, $Z_G(4A) = 4$.

$Z_G(2A) = \mathrm{End}(\underbrace{\mathbb{F}[x]/x + 1}_{M_1} \oplus \underbrace{\mathbb{F}[x]/(x + 1)^2}_{M_2})^\times$. Then $M_1 = \mathbb{F}$ and, by a change of variables $\varepsilon = x + 1$, $M_2 = \mathbb{F}[\varepsilon]/\varepsilon^2$.

Now observe $\mathrm{End}(M_1) = \mathrm{End}(\mathbb{F}) = \mathbb{F}$ and also $\mathrm{End}(M_2) = \mathrm{End}(\mathbb{F}[\varepsilon]/\varepsilon^2) = \mathbb{F}[\varepsilon]/\varepsilon^2$.

$\mathrm{Hom}(M_2, M_1) = \mathrm{Hom}(\mathbb{F}[\varepsilon]/\varepsilon^2, \mathbb{F}) = \mathbb{F}$, since we may map the single generator of $\mathbb{F}[\varepsilon]/\varepsilon^2$ to *either* 0 or 1. $\mathrm{Hom}(M_1, M_2) = \mathrm{Hom}(\mathbb{F}, \mathbb{F}[\varepsilon]/\varepsilon^2) = \varepsilon\mathbb{F}[\varepsilon]/\varepsilon^2$.

$$\mathrm{End}_{\mathbb{F}[\varepsilon]}(F \oplus \mathbb{F}[\varepsilon]/\varepsilon)^\times = \left\{ \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} : f_{11}, f_{12} \in \mathbb{F}, f_{21} \in \varepsilon\mathbb{F}[\varepsilon]/\varepsilon^2, f_{22} \in \mathbb{F}[\varepsilon]/\varepsilon^2 \right\}$$

so we can compute the cardinality End $= 2^2 * 2 * 4 = 32$.

Generally, let M_1, M_2 be R-modules (for commutative R) and $M = M_1 \oplus M_2$. Then consider $f \in \text{End}(M_1 \oplus M_2)$. We have $f(m_1, m_2) = (f_1(m_1, m_2), f_2(m_1, m_2))$, where $f_1(m_1, m_2) \in M_1$ and $f_2(m_1, m_2) \in M_2$.

Then $f_1(m_1, m_2) = f_1(m_1, 0) + f_1(0, m_2)$. Define $f_{11} : M_1 \to M_1$ by $f_{11}(m_1) = f_1(m_1, 0)$ and $f_{12} : M_2 \to M_1$ by $f_{12}(m_2) = f_1(0, m_2)$. Note that $f_{11} \in \text{Hom}(M_1, M_1)$ and $f_{12} \in \text{Hom}(M_2, M_1)$.

Similarly, we write $f_2(m_1, m_2) = f_{21}(m_1) + f_{22}(m_2)$ for $f_{22} \in \text{Hom}(M_2, M_2)$ and $f_{21} \in \text{Hom}(M_1, M_2)$. We can then express

$$\text{End}_R(M_1 \oplus M_2) = \left\{ \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} : f_{ij} \in \text{Hom}(M_j, M_i) \right\}$$

> **3.15**
>
> The map $f \mapsto f(1)$ gives an isomorphism over $\text{End}_{\mathbb{F}[x]}(\mathbb{F}[x]/d_1(x)) \to \mathbb{F}[x]/d_1(x)$. Its inverse is $f_a(d) = a \cdot d \hookleftarrow a$

We reconsider our calculation of $2A$. We have $V \cong \mathbb{F}[x]/(x+1) \oplus \mathbb{F}[x]/(x+1)^2 = \mathbb{F} \oplus \mathbb{F}[x]/(x+1)^2 = \mathbb{F} \oplus \mathbb{F}[\varepsilon]/\varepsilon^2$.

V then has two generators, $e_1 = (1, 0)$ and $e_2 = (0, 1)$. Let $f \in \text{End}_{\mathbb{F}[\varepsilon]}(V)$. Then $f(e_1) = ae_1 + \beta e_2$, where $a \in \mathbb{F}$, $\beta \in \mathbb{F}[\varepsilon]/\varepsilon^2$. Then $\varepsilon e_1 = 0$, so $0 = f(\varepsilon e_1) = \varepsilon f(e_1) = \varepsilon a e_1 + \varepsilon \beta e_2 = \varepsilon \beta e_2 = 0 \implies \varepsilon \beta = 0$ in $\mathbb{F}[\varepsilon]/\varepsilon^2$. Hence, $\beta = \varepsilon b$ for some $b \in \mathbb{F}$.

We write, now, $f(e_1) = ae_1 + b\varepsilon e_2$, with $a, b \in \mathbb{F}$. We also write $f(e_2) = ce_1 + \delta e_2$ for $c \in \mathbb{F}$, $\delta \in \mathbb{F}[\varepsilon]$. Then we have

$$R = \text{End}_{\mathbb{F}[\varepsilon]}(V) = \left\{ \begin{pmatrix} a & c \\ b\varepsilon & \delta \end{pmatrix} : a, b \in \mathbb{F}, \delta = d_1 + d_2\varepsilon \in \mathbb{F}[\varepsilon]/\varepsilon^2 \right\}$$

$\implies$ $\#R = 32$. We'd like to isolate only its invertible elements. After some simplification, an arbitrary multiplication of elements in R looks like:

$$\begin{pmatrix} a & c \\ b\varepsilon & \delta \end{pmatrix} \begin{pmatrix} a' & c' \\ b'\varepsilon & \delta' \end{pmatrix} = \begin{pmatrix} aa' & ac' + cd_1' \\ a'b\varepsilon + b'd_1\varepsilon & bc'\varepsilon + \delta\delta' \end{pmatrix}$$

so the notion is well-defined. Consider

$$\mathbb{F}[\varepsilon]/\varepsilon^2 = V \to V/\varepsilon V =: \overline{V}$$

note that $V/\varepsilon V = \mathbb{F} \oplus \mathbb{F}$, noting $V = \mathbb{F} \oplus \mathbb{F}[\varepsilon]/\varepsilon^2$. Then, if $f : V \to V$ is invertible, $\overline{f} : \overline{V} \to \overline{V}$, where $\overline{f}$ is represented by $\begin{pmatrix} a & c \\ 0 & d_1 \end{pmatrix}$, so $\overline{f}$ is invertible $\iff a = d_1 = 1$. Hence,

$$\mathrm{End}(V)^\times \subseteq \left\{ \begin{pmatrix} 1 & c \\ b\varepsilon & 1 + d_2\varepsilon \end{pmatrix} : c, b, d_2 \in \mathbb{F} \right\} \cong D_8(!)$$

Our final table for $\mathrm{GL}_3(\mathbb{F}_2)$ is as follows:

Class	#$Z(g)$	#Class
$3A$	3	56
$7A$	7	24
$7B$	7	24
$4A$	4	42
$2A$	8	21
$1A$	168	1

Note that, if $\mathbb{F}$ is any field at all, then

$$\mathrm{End}_{\mathbb{F}[x]}(\mathbb{F}[x]/f_1 \oplus \mathbb{F}[x]/f_2) \cong \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, a_{ij} \in \mathrm{Hom}_{\mathbb{F}[x]}(M_j, M_i) \right\}$$

where $M_1 = \mathbb{F}[x]/f_1$ and $M_2 = \mathbb{F}[x]/f_2$.

3.16

$$\mathrm{Hom}_{\mathbb{F}[x]}\left(\mathbb{F}[x]/f_1, \mathbb{F}[x]/f_2\right) = \frac{f_2}{\gcd(f_1, f_2)} \cdot \mathbb{F}[x]/f_2$$

In particular, ... = 0 if $\gcd(f_1, f_2) = 1$, and ... = $\frac{f_2}{f_1}\mathbb{F}[x]/f_2$ if $f_1|f_2$, and ... = $\mathbb{F}[x]/f_2$ if $f_2|f_1$.