

# Algebra Notes

D. Zack Garza

January 6, 2020

## Contents

<b>1</b>	<b>Group Theory</b>	<b>2</b>
1.1	Big List of Notation . . . . .	2
1.2	Basics . . . . .	2
1.3	Finitely Generated Abelian Groups . . . . .	3
1.4	The Symmetric Group . . . . .	4
1.5	Counting Theorems . . . . .	5
1.5.1	Examples of Orbit-Stabilizer . . . . .	6
1.5.2	Sylow Theorems . . . . .	7
1.5.3	Sylow 1 (Cauchy for Prime Powers) . . . . .	7
1.5.4	Sylow 2 (Sylows are Conjugate) . . . . .	7
1.5.5	Sylow 3 (Numerical Constraints) . . . . .	7
1.6	Products . . . . .	8
1.7	Isomorphism Theorems . . . . .	8
1.8	Special Classes of Groups . . . . .	9
1.9	Series of Groups . . . . .	11
<b>2</b>	<b>Rings</b>	<b>11</b>
2.1	Definitions . . . . .	11
2.2	Nontrivial Properties . . . . .	13
2.3	Ideals . . . . .	13
2.3.1	Maximal and Prime Ideals . . . . .	13
2.3.2	Nilradical and Jacobson Radical . . . . .	13
2.3.3	Zorn's Lemma . . . . .	14
<b>3</b>	<b>Fields</b>	<b>15</b>
3.1	Finite Fields . . . . .	15
3.2	Galois Theory . . . . .	16
3.2.1	Lemmas About Towers . . . . .	16
3.2.2	Examples . . . . .	18
3.3	Cyclotomic Polynomials . . . . .	19
<b>4</b>	<b>Modules</b>	<b>20</b>
4.1	General Modules . . . . .	20
4.2	Classification of Modules over a PID . . . . .	20
4.3	Minimal / Characteristic Polynomials . . . . .	20

4.4	Canonical Forms . . . . .	21
4.4.1	Rational Canonical Form . . . . .	21
4.4.2	Jordan Canonical Form . . . . .	22
4.5	Using Canonical Forms . . . . .	22
4.6	Diagonalizability . . . . .	23
4.7	Matrix Counterexamples . . . . .	24
4.8	Miscellaneous . . . . .	24

# 1 Group Theory

## 1.1 Big List of Notation

$C(x) =$	$\{g \in G \mid gxg^{-1} = x\}$	$\subseteq G$	Centralizer
$C_G(h) =$	$\{ghg^{-1} \mid g \in G\}$	$\subseteq G$	Conjugacy Class
$Gx =$	$\{g.x \mid x \in X\}$	$\subseteq X$	Orbit
$G_x =$	$\{g \in G \mid g.x = x\}$	$\subseteq G$	Stabilizer
$X_g =$	$\{x \in X \mid \forall g \in G, g.x = x\}$	$\subseteq X$	Fixed Points
$Z(G) =$	$\{x \in G \mid \forall g \in G, gxg^{-1} = x\}$	$\subseteq G$	Center
$\text{Inn}(G) =$	$\{\phi_g(x) = gxg^{-1}\}$	$\subseteq \text{Aut}(G)$	Inner Aut.
$\text{Out}(G) =$	$\text{Aut}(G)/\text{Inn}(G)$	$\hookrightarrow \text{Aut}(G)$	Outer Aut.
$N(H) =$	$\{g \in G \mid gHg^{-1} = H\}$	$\subseteq G$	Normalizer

## 1.2 Basics

**Definition (Centralizer):**

$$C_G(H) = \{g \in G \mid ghg^{-1} = h \forall h \in H\}$$

**Definition (Normalizer):**

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

**Lemma:**  $C_G(H) \trianglelefteq N_G(H)$

**Lemma:** The size of the conjugacy class of  $H$  is the index of its centralizer, i.e.

$$|\{gHg^{-1} \mid g \in G\}| = [G : C_G(H)].$$

Proof: Orbit-stabilizer.

**Lemma (“The Fundamental Theorem of Cosets”):**

$$aH = bH \iff a^{-1}b \in H \text{ or } aH \cap bH = \emptyset$$

**Definition:**  $[x, y] = x^{-1}y^{-1}xy$  is the **commutator**, and  $[G, G] := \{[x, y] \mid x, y \in G\}$  is the **commutator subgroup**.

**Lemma:**

$$[G, G] \leq H \text{ and } H \trianglelefteq G \implies G/H \text{ is abelian.}$$

**Lemmas:**

- Every subgroup of a cyclic group is itself cyclic.
- Intersections of subgroups are still subgroups
  - Intersections of distinct coprime-order subgroups are trivial
  - Intersections of subgroups of the same prime order are either trivial or equality
- The Quaternion group has only one element of order 2, namely  $-1$ .
  - They also have the presentation

$$\begin{aligned} Q &= \langle x, y, z \mid x^2 = y^2 = z^2 = xyz = -1 \rangle \\ &= \langle x, y \mid x^4 = y^4 = e, x^2 = y^2, yxy^{-1} = x^{-1} \rangle. \end{aligned}$$

- A dihedral group always has a presentation of the form

$$D_n = \langle x, y \mid x^n = y^2 = (xy)^2 = e \rangle,$$

yielding at least 2 distinct elements of order 2.

### 1.3 Finitely Generated Abelian Groups

Invariant factor decomposition:

$$G \cong \mathbb{Z}^r \times \prod_{j=1}^m \mathbb{Z}/(n_j) \quad \text{where } n_1 \mid \cdots \mid n_m.$$

**Going from invariant divisors to elementary divisors:**

- Take prime factorization of each factor
- Split into coprime pieces

*Example:*

$$\begin{aligned} &\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2^3 \cdot 5^2 \cdot 7) \\ &\cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2^3) \oplus \mathbb{Z}/(5^2) \oplus \mathbb{Z}/(7) \end{aligned}$$

**Going from elementary divisors to invariant factors:**

- Bin up by primes occurring (keeping exponents)
- Take highest power from each prime as *last* invariant factor
- Take highest power from all remaining primes as next, etc

*Example:* Given the invariant factor decomposition

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}, .$$

$p = 2$	$p = 3$	$p = 5$
2, 2, 2	3, 3	$5^2$

$$\implies n_m = 5^2 \cdot 3 \cdot 2$$

$p = 2$	$p = 3$	$p = 5$
2, 2	3	$\emptyset$

$$\implies n_{m-1} = 3 \cdot 2$$

$p = 2$	$p = 3$	$p = 5$
2	$\emptyset$	$\emptyset$

$$\implies n_{m-2} = 2$$

and thus

$$G \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(3 \cdot 2) \oplus \mathbb{Z}/(5^2 \cdot 3 \cdot 2).$$

## 1.4 The Symmetric Group

**Definitions:**

- A cycle is **even**  $\iff$  product of an *even* number of transpositions.
  - A cycle of even *length* is **odd**
  - A cycle of odd *length* is **even**

**Definition** The **alternating group** is the subgroup of **even** permutations, i.e.  $A_n := \left\{ \sigma \in S_n \mid \text{sign}(\sigma) = 1 \right\}$  where  $\text{sign}(\sigma) = (-1)^m$  where  $m$  is the number of cycles of even length.

*Corollary:* Every  $\sigma \in A_n$  has an even number of *odd* cycles (i.e. an even number of *even-length* cycles).

*Example:*

$$A_4 = \{\text{id}, \\ (1, 3)(2, 4), (1, 2)(3, 4), (1, 4)(2, 3), \\ (1, 2, 3), (1, 3, 2), \\ (1, 2, 4), (1, 4, 2), \\ (1, 3, 4), (1, 4, 3), \\ (2, 3, 4), (2, 4, 3)\}.$$

**Lemmas:**

- The transitive subgroups of  $S_3$  are  $S_3, A_3$
- The transitive subgroups of  $S_4$  are  $S_4, A_4, D_4, \mathbb{Z}_2^2, \mathbb{Z}_4$ .
- $S_4$  has two normal subgroups:  $A_4, \mathbb{Z}_2^2$ .
- $S_{n \geq 5}$  has one normal subgroup:  $A_n$ .
- $Z(S_n) = 1$  for  $n \geq 3$
- $Z(A_n) = 1$  for  $n \geq 4$
- $[S_n, S_n] = A_n$
- $[A_4, A_4] \cong \mathbb{Z}_2^2$
- $[A_n, A_n] = A_n$  for  $n \geq 5$ , so  $A_{n \geq 5}$  is nonabelian.
- $A_{n \geq 5}$  is *simple*.

## 1.5 Counting Theorems

**Lagrange's Theorem:**

$$H \leq G \implies |H| \mid |G|.$$

*Corollary:* The order of every element divides the size of  $G$ , i.e.

$$g \in G \implies o(g) \mid o(G) \implies g^{|G|} = e.$$

**Warning:** There does **not** necessarily exist  $H \leq G$  with  $|H| = n$  for every  $n \mid |G|$ .  
Counterexample:  $|A_4| = 12$  but has no subgroup of order 6.

**Cauchy's Theorem:**

For every prime  $p$  dividing  $|G|$ , there is an element (and thus a subgroup) of order  $p$ .

This is a partial converse to Lagrange's theorem, and strengthened by Sylow's theorem.

**Notation:** For a group  $G$  acting on a set  $X$ ,

- $G \cdot x = \{g \curvearrowright x \mid g \in G\} \subseteq X$  is the orbit
- $G_x = \{g \in G \mid g \curvearrowright x = x\} \subseteq G$  is the stabilizer
- $X/G \subset \mathcal{P}(X)$  is the set of orbits

- $X^g = \{x \in X \mid g \curvearrowright x = x\} \subseteq X$  are the fixed points

**Orbit-Stabilizer:**

$$|G \cdot x| = [G : G_x] = |G|/|G_x| \quad \text{if } G \text{ is finite}$$

Mnemonic:  $G/G_x \cong G \cdot x$ .

### 1.5.1 Examples of Orbit-Stabilizer

1. Let  $G$  act on itself by conjugation.

- $G \cdot x$  is the **conjugacy class** of  $x$
- $G_x = Z(x) := C_G(x) = \{g \mid [g, x] = e\}$ , the **centralizer** of  $x$ .
- $G^g$  (the fixed points) is the **center**  $Z(G)$ .

*Corollary:* The number of conjugates of an element (i.e. the size of its conjugacy class) is the index of its centralizer,  $[G : C_G(x)]$ .

*Corollary:* the **Class Equation**:

$$|G| = |Z(G)| + \sum_{\substack{\text{One } x_i \text{ from} \\ \text{each conjugacy} \\ \text{class}}} [G : Z(x_i)]$$

1. Let  $G$  act on  $S$ , its set of *subgroups*, by conjugation.

- $G \cdot H = \{gHg^{-1}\}$  is the **set of conjugate subgroups** of  $H$
- $G_H = N_G(H)$  is the **normalizer** of  $H$  in  $G$
- $S^G$  is the set of **normal subgroups** of  $G$

*Corollary:* Given  $H \leq G$ , the number of conjugate subgroups is  $[G : N_G(H)]$ .

1. For a fixed proper subgroup  $H < G$ , let  $G$  act on its cosets  $G/H = \{gH \mid g \in G\}$  by left-multiplication.

- $G \cdot gH = G/H$ , i.e. this is a *transitive* action.
- $G_{gH} = gHg^{-1}$  is a *conjugate subgroup* of  $H$
- $(G/H)^G = \emptyset$

*Application:* If  $G$  is simple,  $H < G$  proper, and  $[G : H] = n$ , then there exists an injective map  $\phi : G \hookrightarrow S_n$ .

*Proof:* This action induces  $\phi$ ; it is nontrivial since  $gH \neq H$  for all  $g$  implies  $H = G$ ;  $\ker \phi \trianglelefteq G$  and  $G$  simple implies  $\ker \phi = 1$ .

**Burnside's Formula:**

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

### 1.5.2 Sylow Theorems

**Notation:** For any  $p$ , let  $\text{Syl}_p(G)$  be the set of Sylow- $p$  subgroups of  $G$ .

Write

- $|G| = p^n m$  where  $(m, p) = 1$ ,
- $S_p$  a Sylow- $p$  subgroup, and
- $n_p$  the number of Sylow- $p$  subgroups.

**Definition:** A  $p$ -group is a group  $G$  such that every element is order  $p^k$  for some  $k$ . If  $G$  is a finite  $p$ -group, then  $|G| = p^j$  for some  $j$ .

**Lemma:**  $p$ -groups have nontrivial centers.

Some useful facts:

- Coprime order subgroups are disjoint, or more generally  $\mathbb{Z}_p, \mathbb{Z}_q \subset G \implies \mathbb{Z}_p \cap \mathbb{Z}_q = \mathbb{Z}_{(p,q)}$ .
- The Chinese Remainder theorem:  $(p, q) = 1 \implies \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$

### 1.5.3 Sylow 1 (Cauchy for Prime Powers)

$\forall p^n$  dividing  $|G|$  there exists a subgroup of size  $p^n$ .

If  $|G| = \prod p_i^{\alpha_i}$ , then there exist subgroups of order  $p_i^{\beta_i}$  for every  $i$  and every  $0 \leq \beta_i \leq \alpha_i$ . In particular, Sylow  $p$ -subgroups always exist.

### 1.5.4 Sylow 2 (Sylows are Conjugate)

All sylow- $p$  subgroups  $S_p$  are conjugate, i.e.

$$S_p^1, S_p^2 \in \text{Syl}_p(G) \implies \exists g \text{ such that } gS_p^1g^{-1} = S_p^2.$$

**Corollary:**  $n_p = 1 \iff S_p \trianglelefteq G$

### 1.5.5 Sylow 3 (Numerical Constraints)

1.  $n_p \mid m$  (in particular,  $n_p \leq m$ ),
2.  $n_p \equiv 1 \pmod{p}$ ,
3.  $n_p = [G : N_G(S_p)]$  where  $N_G$  is the normalizer.

**Corollary:**  $p$  does not divide  $n_p$ .

**Lemma:** Every  $p$ -subgroup of  $G$  is contained in a Sylow  $p$ -subgroup.

*Proof:* Let  $H \leq G$  be a  $p$ -subgroup. If  $H$  is not *properly* contained in any other  $p$ -subgroup, it is a Sylow  $p$ -subgroup by definition. Otherwise, it is contained in some  $p$ -subgroup  $H^1$ . Inductively this yields a chain  $H \subsetneq H^1 \subsetneq \dots$ , and by Zorn's lemma  $H := \bigcup_i H^i$  is maximal and thus a Sylow  $p$ -subgroup.

**Fratini's Argument:** If  $H \trianglelefteq G$  and  $P \in \text{Syl}_p(G)$ , then  $HN_G(P) = G$  and  $[G : H]$  divides  $|N_G(P)|$ .

## 1.6 Products

**Characterizing direct products:**  $G \cong H \times K$  when

- $G = HK = \{hk \mid h \in H, k \in K\}$
- $H \cap K = \{e\} \subset G$
- $H, K \trianglelefteq G$

Can relax to only  $H \trianglelefteq G$  to get a semidirect product instead

**Characterizing semidirect products:**  $G = N \rtimes_{\psi} H$  when

- $G = NH$
- $N \trianglelefteq G$
- $H \curvearrowright N$  by conjugation via a map

$$\begin{aligned} \psi : H &\rightarrow \text{Aut}(N) \\ h &\mapsto h(\cdot)h^{-1}. \end{aligned}$$

### Useful Facts

- If  $\sigma \in \text{Aut}(H)$ , then  $N \rtimes_{\psi} H \cong N \rtimes_{\psi \circ \sigma} H$ .
- $\text{Aut}(\mathbb{Z}/(p)^n) \cong \text{GL}(n, \mathbb{F}_p)$ 
  - If this occurs in a semidirect product, it suffices to consider similarity classes of matrices (i.e. just use canonical forms)
- $\text{Aut}(\mathbb{Z}/(n)) \cong \mathbb{Z}/(n)^{\times} \cong \mathbb{Z}/(\varphi(n))$  where  $\varphi$  is the totient function.
  - $\varphi(p^k) = p^{k-1}(p-1)$
- If  $G, H$  have coprime order then  $\text{Aut}(G \oplus H) \cong \text{Aut}(G) \oplus \text{Aut}(H)$ .

## 1.7 Isomorphism Theorems

**Lemma:** If  $H, K \leq G$  and  $H \leq N_G(K)$  (or  $K \trianglelefteq G$ ) then  $HK \leq G$  is a subgroup.

Note that this implies that  $HK$  is not always a subgroup.

**Diamond Theorem / 2nd Isomorphism Theorem:**

If  $S \leq G$  and  $N \trianglelefteq G$ , then

$$\frac{SN}{N} \cong \frac{S}{S \cap N} \quad \text{and} \quad |SN| = \frac{|S||N|}{|S \cap N|}$$





Mnemonic:

Note: for this to make sense, we also have

- $SN \leq G$ ,
- $S \cap N \leq S$ ,

### Cancellation / 3rd Isomorphism Theorem

If  $H, K \leq G$  with  $H \leq K$ , then

$$\frac{G/H}{G/K} \cong \frac{G}{K}$$

Note: for this to make sense, we also have  $G/K \leq G/H$ .

**The Correspondence Theorem / 4th Isomorphism Theorem:** Suppose  $N \leq G$ , then there exists a correspondence:

$$\begin{aligned} \left\{ H < G \mid N \subseteq H \right\} &\iff \left\{ H \mid H < \frac{G}{N} \right\} \\ \left\{ \begin{array}{l} \text{Subgroups of } G \\ \text{containing } N \end{array} \right\} &\iff \left\{ \begin{array}{l} \text{Subgroups of the} \\ \text{quotient } G/N \end{array} \right\}. \end{aligned}$$

In words, subgroups of  $G$  containing  $N$  correspond to subgroups of the quotient group  $G/N$ . This is given by the map  $H \mapsto H/N$ .

Note:  $N \leq G$  and  $N \subseteq H < G \implies N \leq H$ .

## 1.8 Special Classes of Groups

**Definition:** The “**2 out of 3 property**” is satisfied by a class of groups  $\mathcal{C}$  iff whenever  $G \in \mathcal{C}$ , then  $N, G/N \in \mathcal{C}$  for any  $N \leq G$ .

**Definition:** If  $|G| = p^k$ , then  $G$  is a **p-group**.

**Facts about p-groups:**

- If  $k = 1$  then  $G$  is cyclic
- If  $k = 2$ , then  $G \cong \mathbb{Z}/(p)^2$  or  $\mathbb{Z}/(p^2)$ .
- p-groups have nontrivial centers
  - Proof: Use class equation.
- Every normal subgroup is contained in the center
- Normalizers grow
- Every maximal is normal
- Every maximal has index  $p$
- p-groups are *nilpotent*
- p-groups are *solvable*

**Facts about other special order groups:**

- $|G| = pq$ : Two possibilities. By cases:
  - If  $p$  divides  $q - 1$ , two cases:
    - \*  $G \cong \mathbb{Z}/(pq)$  or  $\mathbb{Z}(p) \times \mathbb{Z}/(q)$
  - Otherwise,  $G \cong \mathbb{Z}/(pq)$

Proof: Sylow theorems. Note: Such groups are never simple.

- $|G| = p^2q$ :

**Definition:** A group  $G$  is **simple** iff  $H \trianglelefteq G \implies H = \{e\}, G$ , i.e. it has no non-trivial proper subgroups.

**Lemma:** If  $G$  is *not* simple, then for any  $N \trianglelefteq G$ , it is the case that  $G \cong E$  for an extension of the form  $N \rightarrow E \rightarrow G/N$ .  $>$

**Definition:** A group  $G$  is **solvable** iff  $G$  has a terminating normal series with abelian factors, i.e.

$$G \rightarrow G^1 \rightarrow \cdots \rightarrow \{e\} \text{ with } G^i/G^{i+1} \text{ abelian for all } i.$$

**Lemmas:**

- $G$  is solvable iff  $G$  has a terminating *derived series*.
- Solvable groups satisfy the 2 out of 3 property
- Abelian  $\implies$  solvable
- Every group of order less than 60 is solvable.

**Definition:** A group  $G$  is **nilpotent** iff  $G$  has a terminating central series, upper central series, or lower central series.

Moral: the adjoint map is nilpotent.

**Lemma:** For  $G$  a finite group, TFAE:

- $G$  is nilpotent

- Normalizers grow (i.e.  $H < N_G(H)$  whenever  $H$  is proper)
- Every Sylow-p subgroup is normal
- $G$  is the direct product of its Sylow p-subgroups
- Every maximal subgroup is normal
- $G$  has a terminating *Lower* Central Series
- $G$  has a terminating *Upper* Central Series

**Lemmas:**

- $G$  nilpotent  $\implies G$  solvable
- Nilpotent groups satisfy the 2 out of 3 property.
- $G$  has normal subgroups of order  $d$  for *every*  $d$  dividing  $|G|$
- $G$  nilpotent  $\implies Z(G) \neq 0$
- Abelian  $\implies$  nilpotent
- p-groups  $\implies$  nilpotent

## 1.9 Series of Groups

**Definition:** A **normal series** of a group  $G$  is a sequence  $G \rightarrow G^1 \rightarrow G^2 \rightarrow \dots$  such that  $G^{i+1} \trianglelefteq G_i$  for every  $i$ .

**Definition** A **composition series** of a group  $G$  is a finite normal series such that  $G^{i+1}$  is a *maximal proper* normal subgroup of  $G^i$ .

**Theorem (Jordan-Hölder):** Any two composition series of a group have the same length and isomorphic factors (up to permutation).<sup>1</sup>

**Definition** A **derived series** of a group  $G$  is a normal series  $G \rightarrow G^1 \rightarrow G^2 \rightarrow \dots$  where  $G^{i+1} = [G^i, G^i]$  is the commutator subgroup.

The derived series terminates iff  $G$  is *solvable*.

**Definition:** A **central series** for a group  $G$  is a terminating normal series  $G \rightarrow G^1 \rightarrow \dots \rightarrow \{e\}$  such that each quotient is **central**, i.e.  $[G, G^i] \leq G^{i-1}$  for all  $i$ .

**Definition:** A **lower central series** is a terminating normal series  $G \rightarrow G^1 \rightarrow \dots \rightarrow \{e\}$  such that  $G^{i+1} = [G^i, G]$

Moral: Iterate the adjoint map  $[\cdot, G]$ .

$G$  is nilpotent  $\iff$  the LCS terminates.

**Definition:** An **upper central series** is a terminating normal series  $G \rightarrow G^1 \rightarrow \dots \rightarrow \{e\}$  such that  $G^1 = Z(G)$  and  $G^{i+1}$  is defined such that  $G^{i+1}/G^i = Z(G^i)$ .

Moral: Iterate taking “higher centers”.

## 2 Rings

### 2.1 Definitions

**Definition:** A ring  $R$  is **simple** iff every ideal  $I \trianglelefteq R$  is either 0 or  $R$ .

**Definition:** An element  $r \in R$  is **irreducible** iff  $r = ab \implies a$  is a unit or  $b$  is a unit.

**Definition:** An element  $r \in R$  is **prime** iff  $ab \mid r \implies a \mid r$  or  $b \mid r$  whenever  $a, b$  are nonzero and not units.

**Definition:**  $\mathfrak{p}$  is a **prime ideal**  $\iff ab \in \mathfrak{p} \implies a \in \mathfrak{p}$  or  $b \in \mathfrak{p}$ .

**Definition:**  $\text{Spec}(R) = \{\mathfrak{p} \trianglelefteq R \mid \mathfrak{p} \text{ is prime}\}$  is the **spectrum** of  $R$ .

**Definition:**  $\mathfrak{m}$  is **maximal**  $\iff I \not\trianglelefteq R \implies I \subseteq \mathfrak{m}$ .

**Definition:**  $\text{Spec}_{\max}(R) = \{\mathfrak{m} \trianglelefteq R \mid \mathfrak{m} \text{ is maximal}\}$  is the **max-spectrum** of  $R$ .

Note: nonstandard notation / definition.

### Lemmas (Quotienting):

- $R/I$  is a domain  $\iff I$  is prime,
- $R/I$  is a field  $\iff I$  is maximal.
- For  $R$  a PID,  $I$  is prime  $\iff I$  is maximal.

### Lemma (Characterizations of Rings):

- $R$  a commutative division ring  $\implies R$  is a field
- $R$  a finite integral domain  $\implies R$  is a field.
- $\mathbb{F}$  a field  $\implies \mathbb{F}[x]$  is a Euclidean domain.
- $\mathbb{F}$  a field  $\implies \mathbb{F}[x]$  is a PID.
- $\mathbb{F}$  is a field  $\iff \mathbb{F}$  is a commutative simple ring.
- $R$  is a UFD  $\iff R[x]$  is a UFD.
- $R$  a PID  $\implies R[x]$  is a UFD
- $R$  a PID  $\implies R$  Noetherian
- $R[x]$  a PID  $\implies R$  is a field.

**Lemma:** Fields  $\subset$  Euclidean domains  $\subset$  PIDs  $\subset$  UFDs  $\subset$  Integral Domains  $\subset$  Rings

- A Euclidean Domain that is not a field:  $\mathbb{F}[x]$  for  $\mathbb{F}$  a field  
– *Proof:* Use previous lemma, and  $x$  is not invertible
- A PID that is not a Euclidean Domain:  $\mathbb{Z}\left[\frac{1 + \sqrt{-19}}{2}\right]$ .  
– *Proof:* complicated.
- A UFD that is not a PID:  $\mathbb{F}[x, y]$ .  
– *Proof:*  $\langle x, y \rangle$  is not principal
- An integral domain that is not a UFD:  $\mathbb{Z}[\sqrt{-5}]$   
– *Proof:*  $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 = 3 \cdot 3$ , where all factors are irreducible (check norm).
- A ring that is not an integral domain:  $\mathbb{Z}/(4)$   
– *Proof:*  $2 \pmod{4}$  is a zero divisor.

**Lemma:** In  $R$  a UFD, an element  $r \in R$  is prime  $\iff r$  is irreducible.

Note: For  $R$  an integral domain, prime  $\implies$  irreducible, but generally not the converse.

*Example of a prime that is not irreducible:*  $x^2 \pmod{(x^2 + x)} \in \mathbb{Q}[x]/(x^2 + x)$ . Check that  $x$  is prime directly, but  $x = x \cdot x$  and  $x$  is not a unit.

*Example of an irreducible that is not prime:*  $3 \in \mathbb{Z}[\sqrt{-5}]$ . Check norm to see irreducibility, but  $3 \mid 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$  and doesn't divide either factor.

**Lemma:** If  $R$  is a PID, then every element in  $R$  has a unique prime factorization.

**Definition:** A nonzero unital ring  $R$  is **semisimple** iff  $R \cong \bigoplus_{i=1}^n M_i$  with each  $M_i$  a simple module.

**Theorem (Artin-Wedderburn):** If  $R$  is a nonzero, unital, *semisimple* ring then  $R \cong \bigoplus_{i=1}^m \text{Mat}(n_i, D_i)$ , a finite sum of matrix rings over division rings.

*Corollary:* If  $M$  is a simple ring over  $R$  a division ring, the  $M$  is isomorphic to a matrix ring.

## 2.2 Nontrivial Properties

**Lemma:** Every  $a \in R$  for a finite ring is either a unit or a zero divisor.

*Proof:* Let  $a \in R$  and define  $\phi(x) = ax$ . If  $\phi$  is injective, then it is surjective, so  $1 = ax$  for some  $x \implies x^{-1} = a$ . Otherwise,  $ax_1 = ax_2$  with  $x_1 \neq x_2 \implies a(x_1 - x_2) = 0$  and  $x_1 - x_2 \neq 0$ , so  $a$  is a zero divisor.

## 2.3 Ideals

### 2.3.1 Maximal and Prime Ideals

**Lemma:** Maximal  $\implies$  prime, but generally not the converse.

*Counterexample:*  $(0) \in \mathbb{Z}$  is prime since  $\mathbb{Z}$  is a domain, but not maximal since it is properly contained in any other ideal.

*Proof:* Suppose  $\mathfrak{m}$  is maximal,  $ab \in \mathfrak{m}$ , and  $b \notin \mathfrak{m}$ . Then there is a containment of ideals  $\mathfrak{m} \subsetneq \mathfrak{m} + (b) \implies \mathfrak{m} + (b) = R$ .  
So

$$1 = m + rb \implies a = am + r(ab),$$

but  $am \in \mathfrak{m}$  and  $ab \in \mathfrak{m} \implies a \in \mathfrak{m}$ . ■

**Lemma:** If  $x$  is not a unit, then  $x$  is contained in some maximal ideal  $\mathfrak{m}$ .

*Proof:* Zorn's lemma.

**Lemma:**  $R/\mathfrak{m}$  is a field  $\iff \mathfrak{m}$  is maximal.

**Lemma:**  $R/\mathfrak{p}$  is an integral domain  $\iff \mathfrak{p}$  is prime.

### 2.3.2 Nilradical and Jacobson Radical

**Definition:**  $\mathfrak{N} := \{x \in R \mid x^n = 0 \text{ for some } n\}$  is the **nilradical** of  $R$ .

**Lemma:** The nilradical is the intersection of all **prime** ideals, i.e.

$$\mathfrak{N}(R) = \bigcap_{\mathfrak{p} \in \text{Spec}(R)} \mathfrak{p}$$

*Proof:*

$$\mathfrak{N} \subseteq \bigcap \mathfrak{p}: x \in \mathfrak{N} \implies x^n = 0 \in \mathfrak{p} \implies x \in \mathfrak{p} \text{ or } x^{n-1} \in \mathfrak{p}.$$

$\mathfrak{N}^c \subseteq \bigcup \mathfrak{p}^c$ : Define  $S = \{I \trianglelefteq R \mid a^n \notin I \text{ for any } n\}$ . Then apply Zorn's lemma to get a maximal ideal  $\mathfrak{m}$ , and maximal  $\implies$  prime.

**Lemma:**  $R/\mathfrak{N}(R)$  has no nonzero nilpotent elements.

*Proof:*

$$\begin{aligned} a + \mathfrak{N}(R) \text{ nilpotent} &\implies (a + \mathfrak{N}(R))^n := a^n + \mathfrak{N}(R) = \mathfrak{N}(R) \\ &\implies a^n \in \mathfrak{N}(R) \\ &\implies \exists \ell \text{ such that } (a^n)^\ell = 0 \\ &\implies a \in \mathfrak{N}(R). \end{aligned}$$

**Definition:** The **Jacobson radical** is the intersection of all **maximal** ideals, i.e.

$$J(R) = \bigcap_{\mathfrak{m} \in \text{Spec}_{\max}} \mathfrak{m}$$

**Lemma:**  $\mathfrak{N}(R) \subseteq J(R)$ .

*Proof:* Maximal  $\implies$  prime, and so if  $x$  is in every prime ideal, it is necessarily in every maximal ideal as well.

### 2.3.3 Zorn's Lemma

**Lemma:** A field has no nontrivial proper ideals.

**Lemma:** If  $I \trianglelefteq R$  is a proper ideal  $\iff I$  contains no units.

$$\text{Proof: } r \in R^\times \cap I \implies r^{-1}r \in I \implies 1 \in I \implies x \cdot 1 \in I \quad \forall x \in R.$$

**Lemma:** If  $I_1 \subseteq I_2 \subseteq \dots$  are ideals then  $\bigcup_j I_j$  is an ideal.

**Example Application of Zorn's Lemma:** Every proper ideal is contained in a maximal ideal.

*Proof:* Let  $0 < I < R$  be a proper ideal, and consider the set

$$S = \{J \mid I \subseteq J < R\}.$$

Note  $I \in S$ , so  $S$  is nonempty. The claim is that  $S$  contains a maximal element  $M$ .

$S$  is a poset, ordered by set inclusion, so if we can show that every chain has an upper bound, we can apply Zorn's lemma to produce  $M$ .

Let  $C \subseteq S$  be a chain in  $S$ , so  $C = \{C_1 \subseteq C_2 \subseteq \dots\}$  and define  $\hat{C} = \bigcup_i C_i$ .

**$\hat{C}$  is an upper bound for  $C$ :**

This follows because every  $C_i \subseteq \hat{C}$ .

**$\hat{C}$  is in  $S$ :**

Use the fact that  $I \subseteq C_i < R$  for every  $C_i$  and since no  $C_i$  contains a unit,  $\hat{C}$  doesn't contain a unit, and is thus proper. ■

### 3 Fields

Let  $k$  denote a field.

**Lemmas:**

- The characteristic of  $\mathbb{F}$  is either 0 or  $p$  a prime.
- All fields are simple rings
- Any homomorphism of fields is either 0 or injective
- If  $L/k$  is algebraic, then  $\min(\alpha, L)$  divides  $\min(\alpha, k)$ .

**Lemma:** Every finite extension is algebraic.

**Eisenstein's Criterion:** If  $f(x) = \sum_{i=0}^n \alpha_i x^i \in \mathbb{Q}[x]$  and  $\exists p$  such that

- $p$  divides every coefficient *except*  $a_n$  and
- $p^2$  does not divide  $a_0$ ,

then  $f$  is irreducible.

**Definition:** For  $R$  a UFD, a polynomial  $p \in R[x]$  is **primitive** iff the greatest common divisors of its coefficients is a unit.

**Gauss' Lemma:** Let  $R$  be a UFD and  $F$  its field of fractions. Then a primitive  $p \in R[x]$  is irreducible in  $R[x] \iff p$  is irreducible in  $F[x]$ .

*Corollary:* A primitive polynomial  $p \in \mathbb{Q}[x]$  is irreducible iff  $p$  is irreducible in  $\mathbb{Z}[x]$ .

#### 3.1 Finite Fields

**Definition:** The prime subfield of a field  $F$  is the subfield generated by 1.

**Lemma (Characterization of Prime Subfields):** The prime subfield of any field is isomorphic to either  $\mathbb{Q}$  or  $\mathbb{F}_p$  for some  $p$ .

**Lemma ("Freshman's Dream"):** If  $\text{char } k = p$  then  $(a + b)^p = a^p + b^p$  and  $(ab)^p = a^p b^p$ .

**Theorem (Construction of Finite Fields):**  $\mathbb{GF}(p^n) \cong \frac{\mathbb{F}_p[x]}{(f)}$  where  $f \in \mathbb{F}_p[x]$  is any irreducible of degree  $n$ , and  $\mathbb{GF}(p^n) \cong \mathbb{F}[\alpha] \cong \text{span}_{\mathbb{F}} \{1, \alpha, \dots, \alpha^{n-1}\}$  for any root  $\alpha$  of  $f$ .

**Lemma (Prime Subfields of Finite Fields):** Every finite field  $F$  is isomorphic to a unique field of the form  $\mathbb{GF}(p^n)$  and if  $\text{char } F = p$ , it has prime subfield  $\mathbb{F}_p$ .

**Lemma (Containment of Finite Fields):**  $\mathbb{GF}(p^\ell) \leq \mathbb{GF}(p^k) \iff \ell$  divides  $k$ .

**Lemma (Identification of Finite Fields as Splitting Fields):**  $\mathbb{GF}(p^n)$  is the splitting field of  $\rho(x) = x^{p^n} - x$ , and the elements are exactly the roots of  $\rho$ .

Every element is a root by Cauchy's theorem, and the  $p^n$  roots are distinct since its derivative is identically  $-1$ .

**Lemma (Splits Product of Irreducibles):** Let  $\rho_n := x^{p^n} - x$ . Then  $f(x) \mid \rho_n(x) \iff \deg f \mid n$  and  $f$  is irreducible.

**Corollary:**  $x^{p^n} - x = \prod f_i(x)$  over all irreducible monic  $f_i \in \mathbb{F}_p[x]$  of degree  $d$  dividing  $n$ .

*Proof:*

$\Leftarrow$  : Suppose  $f$  is irreducible of degree  $d$ . Then  $f \mid x^{p^d} - x$  (consider  $F[x]/\langle f \rangle$ ) and  $x^{p^d} - x \mid x^{p^n} - x \iff d \mid n$ .  
 $\Rightarrow$  :

- $\alpha \in \mathbb{GF}(p^n) \iff \alpha^{p^n} - \alpha = 0$ , so every element is a root of  $\phi_n$  and  $\deg \min(\alpha, \mathbb{F}_p) \mid n$  since  $\mathbb{F}_p(\alpha)$  is an intermediate extension.
- So if  $f$  is an irreducible factor of  $\phi_n$ ,  $f$  is the minimal polynomial of some root  $\alpha$  of  $\phi_n$ , so  $\deg f \mid n$ .  
 $\phi'_n(x) = p^n x^{p^n-1} \neq 0$ , so  $\phi_n$  has distinct roots and thus no repeated factors. So  $\phi_n$  is the product of all such irreducible  $f$ .

**Lemma:** No finite field is algebraically closed.

## 3.2 Galois Theory

**Definition:** A field extension  $L/k$  is **algebraic** iff every  $\alpha \in L$  is the root of some polynomial  $f \in k[x]$ .

**Definition:** Let  $L/k$  be a finite extension. Then TFAE:

- $L/k$  is **normal**.
- Every irreducible  $f \in k[x]$  that has one root in  $L$  has *all* of its roots in  $L$   
 – i.e. every polynomial splits into linear factors
- Every embedding  $\sigma : L \hookrightarrow \bar{k}$  that is a lift of the identity on  $k$  satisfies  $\sigma(L) = L$ .
- If  $L$  is separable:  $L$  is the splitting field of some irreducible  $f \in k[x]$ .

**Definition:** Let  $L/k$  be a field extension,  $\alpha \in L$  be arbitrary, and  $f(x) := \min(\alpha, k)$ . TFAE:

- $L/k$  is **separable**
- $f$  has no repeated factors/roots
- $\gcd(f, f') = 1$ , i.e.  $f$  is coprime to its derivative
- $f' \neq 0$

**Lemma:** If  $\text{char } k = 0$  or  $k$  is finite, then every *algebraic* extension  $L/k$  is separable.

**Definition:**  $\text{Aut}(L/k) = \left\{ \sigma : L \rightarrow L \mid \sigma|_k = \text{id}_k \right\}$ .

**Lemma:** If  $L/k$  is algebraic, then  $\text{Aut}(L/k)$  permutes the roots of irreducible polynomials.

**Lemma:**  $|\text{Aut}(L/k)| \leq [L : k]$  with equality precisely when  $L/k$  is normal.

**Definition:** If  $L/k$  is Galois, we define  $\text{Gal}(L/k) := \text{Aut}(L/k)$ .

### 3.2.1 Lemmas About Towers

Let  $L/F/k$  be a finite tower of field extensions

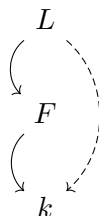
- Multiplicativity:  $[L : k] = [L : F][F : k]$



- $L/k$  normal/algebraic/Galois  $\implies L/F$  normal/algebraic/Galois.
  - *Proof (normal)*:  $\min(\alpha, F) \mid \min(\alpha, k)$ , so if the latter splits in  $L$  then so does the former.
  - *Corollary*:  $\alpha \in L$  algebraic over  $k \implies \alpha$  algebraic over  $F$ .
  - *Corollary*:  $E_1/k$  normal and  $E_2/k$  normal  $\implies E_1E_2/k$  normal and  $E_1 \cap E_2/k$  normal.



- $F/k$  algebraic and  $L/F$  algebraic  $\implies L/k$  algebraic.
- If  $L/k$  is algebraic, then  $F/k$  separable and  $L/F$  separable  $\iff L/k$  separable



- $F/k$  Galois and  $L/F$  Galois  $\implies F/k$  Galois **only if**  $\text{Gal}(L/F) \trianglelefteq \text{Gal}(L/k)$ 
  - $\implies \text{Gal}(F/k) \cong \frac{\text{Gal}(L/k)}{\text{Gal}(L/F)}$



### Common Counterexamples:

- $\mathbb{Q}(\zeta_3, 2^{1/3})$  is normal but  $\mathbb{Q}(2^{1/3})$  is not since the irreducible polynomial  $x^3 - 2$  has only one root in it.

**Definition (Characterizations of Galois Extensions):** Let  $L/k$  be a finite field extension. TFAE:

- $L/k$  is **Galois**
- $L/k$  is finite, normal, and separable.
- $L/k$  is the splitting field of a separable polynomial
- $|\text{Aut}(L/k)| = [L : k]$
- The fixed field of  $\text{Aut}(L/k)$  is exactly  $k$ .

**Fundamental Theorem of Galois Theory:** Let  $L/k$  be a Galois extension, then there is a

correspondence:

$$\begin{aligned} \{\text{Subgroups } H \leq \text{Gal}(L/k)\} &\iff \left\{ \begin{array}{l} \text{Fields } F \text{ such} \\ \text{that } L/F/k \end{array} \right\} \\ H &\rightarrow \{E^H := \text{The fixed field of } H\} \\ \left\{ \text{Gal}(L/F) := \left\{ \sigma \in \text{Gal}(L/k) \mid \sigma(F) = F \right\} \right\} &\leftarrow F. \end{aligned}$$

- This is contravariant with respect to subgroups/subfields.
- $[F : k] = [G : H]$ , so degrees of extensions over the base field correspond to indices of subgroups.
- $[K : F] = |H|$
- $L/F$  is Galois and  $\text{Gal}(K/F) = H$
- $F/k$  is Galois  $\iff H$  is normal, and  $\text{Gal}(F/k) = \text{Gal}(L/k)/H$ .
- The compositum  $F_1 F_2$  corresponds to  $H_1 \cap H_2$ .
- The subfield  $F_1 \cap F_2$  corresponds to  $H_1 H_2$ .

### 3.2.2 Examples

1.  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/(n)^\times$  and is generated by maps of the form  $\zeta_n \mapsto \zeta_n^j$  where  $(j, n) = 1$ .  
I.e., the following map is an isomorphism:

$$\begin{aligned} \mathbb{Z}/(n)^\times &\rightarrow \text{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q}) \\ r \pmod n &\mapsto (\phi_r : \zeta_n \mapsto \zeta_n^r). \end{aligned}$$

2.  $\text{Gal}(\mathbb{GF}(p^n)/\mathbb{GF}(p)) \cong \mathbb{Z}/(n)$ , a cyclic group generated by powers of the Frobenius automorphism:

$$\begin{aligned} \varphi_p : \mathbb{GF}(p^n) &\rightarrow \mathbb{GF}(p^n) \\ x &\mapsto x^p. \end{aligned}$$

**Lemma:** Every quadratic extension is Galois.

**Lemma:** If  $K$  is the splitting field of an irreducible polynomial of degree  $n$ , then  $\text{Gal}(K/\mathbb{Q}) \leq S_n$  is a transitive subgroup.

Corollary:  $n$  divides the order  $|\text{Gal}(K/\mathbb{Q})|$ .

**Definition:** TFAE

- $k$  is a **perfect** field.
- Every irreducible polynomial  $p \in k[x]$  is separable
- Every finite extension  $F/k$  is separable.
- If  $\text{char } k > 0$ , the Frobenius is an automorphism of  $k$ .

**Theorem:**

- If  $\text{char } k = 0$  or  $k$  is finite, then  $k$  is perfect.
- $k = \mathbb{Q}, \mathbb{F}_p$  are perfect, and any finite normal extension is Galois.
- Every splitting field of a polynomial over a perfect field is Galois.

**Lemma (Composite Extensions):** If  $F/k$  is finite and Galois and  $L/k$  is arbitrary, then  $FL/L$  is Galois and

$$\text{Gal}(FL/L) = \text{Gal}(F/F \cap L) \subset \text{Gal}(F/k).$$

### 3.3 Cyclotomic Polynomials

**Definition:** Let  $\zeta_n = e^{2\pi i/n}$ , then

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (k,n)=1}}^n (x - \zeta_n^k),$$

which is a product over primitive roots of unity.

**Lemma:**  $\deg \Phi_n(x) = \phi(n)$  for  $\phi$  the totient function.

**Computing  $\Phi_n$ :**

1.

$$\Phi_n(z) = \prod_{d|n, d>0} (z^d - 1)^{\mu(\frac{n}{d})}$$

where

$$\mu(n) \equiv \begin{cases} 0 & \text{if } n \text{ has one or more repeated prime factors} \\ 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes,} \end{cases}$$

2.

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \implies \Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d < n}} \Phi_d(x)},$$

so just use polynomial long division.

**Lemma:**

$$\begin{aligned} \Phi_p(x) &= x^{p-1} + x^{p-2} + \cdots + x + 1 \\ \Phi_{2p}(x) &= x^{p-1} - x^{p-2} + \cdots - x + 1. \end{aligned}$$

**Lemma:**

$$k \mid n \implies \Phi_{nk}(x) = \Phi_n(x^k)$$

**Definition:** An extension  $F/k$  is **simple** if  $F = k[\alpha]$  for a single element  $\alpha$ .

**Theorem (Primitive Element):** Every finite separable extension is simple.

**Corollary:**  $\mathbb{GF}(p^n)$  is a simple extension over  $\mathbb{F}_p$ .

## 4 Modules

### 4.1 General Modules

**Definition:** A module is **simple** iff it has no nontrivial proper submodules.

**Definition:** A **free** module is a module with a basis (i.e. a spanning, linearly independent set).

*Example:*  $\mathbb{Z}/(6)$  is a  $\mathbb{Z}$ -module that is *not* free.

**Definition:** A module  $M$  is **projective** iff  $M$  is a direct summand of a free module  $F = M \oplus \cdots$ .

Free implies projective, but not the converse.

**Definition:** A sequence of homomorphisms  $0 \xrightarrow{d_1} A \xrightarrow{d_2} B \xrightarrow{d_3} C \rightarrow 0$  is *exact* iff  $\text{im } d_i = \ker d_{i+1}$ .

**Lemma:** If  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  is a short exact sequence, then

- $C$  free  $\implies$  the sequence splits
- $C$  projective  $\implies$  the sequence splits
- $A$  injective  $\implies$  the sequence splits

Moreover, if this sequence splits, then  $B \cong A \oplus C$ .

### 4.2 Classification of Modules over a PID

Let  $M$  be a finitely generated modules over a PID  $R$ . Then there is an invariant factor decomposition

$$M \cong F \bigoplus R/(r_i) \quad \text{where } r_1 \mid r_2 \mid \cdots,$$

and similarly an elementary divisor decomposition.

### 4.3 Minimal / Characteristic Polynomials

Fix some notation:

$\min_A(x)$  : The minimal polynomial of  $A$

$\chi_A(x)$  : The characteristic polynomial of  $A$ .

**Definition:** The minimal polynomial is the unique polynomial  $\min_A(x)$  of minimal degree such that  $\min_A(A) = 0$ .

**Definition:** The **characteristic polynomial** of  $A$  is given by

$$\chi_A(x) = \det(A - xI) = \det(SNF(A - xI)).$$

*Useful lemma:* If  $A$  is upper triangular, then  $\det(A) = \prod_i a_{ii}$

**Theorem (Cayley-Hamilton):** The minimal polynomial divides the characteristic polynomial, and in particular  $\chi_A(A) = 0$ .

**Lemma:** Writing

$$\begin{aligned}\min_A(x) &= \prod (x - \lambda_i)^{a_i} \\ \chi_A(x) &= \prod (x - \lambda_i)^{b_i}\end{aligned}$$

- $a_i \leq b_i$
- The roots both polynomials are precisely the eigenvalues of  $A$ .

*Proof:* By Cayley-Hamilton,  $\min_A$  divides  $\chi_A$ . Every  $\lambda_i$  is a root of  $\mu_M$ :

Let  $(\mathbf{v}_i, \lambda_i)$  be a nontrivial eigenpair. Then by linearity,

$$\min_A(\lambda_i)\mathbf{v}_i = \min_A(A)\mathbf{v}_i = \mathbf{0},$$

which forces  $\min_A(\lambda_i) = 0$ .

**Definition:** Two matrices  $A, B$  are **similar** (i.e.  $A = PBP^{-1}$ )  $\iff A, B$  have the same Jordan Canonical Form (JCF).

**Definition:** Two matrices  $A, B$  are **equivalent** (i.e.  $A = PBQ$ )  $\iff$

- They have the same rank,
- They have the same invariant factors, *and*
- They have the same (JCF)

**Finding the minimal polynomial:**

Let  $m(x)$  denote the minimal polynomial  $A$ .

1. Find the characteristic polynomial  $\chi(x)$ ; this annihilates  $A$  by Cayley-Hamilton. Then  $m(x) \mid \chi(x)$ , so just test the finitely many products of irreducible factors.
2. Pick any  $\mathbf{v}$  and compute  $T\mathbf{v}, T^2\mathbf{v}, \dots, T^k\mathbf{v}$  until a linear dependence is introduced. Write this as  $p(T) = 0$ ; then  $\min_A(x) \mid p(x)$ .

**Definition:** Given a monic  $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1} + x^n$ , the **companion matrix** of  $p$  is given by

$$C_p := \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{bmatrix}.$$

## 4.4 Canonical Forms

### 4.4.1 Rational Canonical Form

Corresponds to the **Invariant Factor Decomposition** of  $T$ .

**Lemma:**  $RCF(A)$  is a block matrix where each block is the companion matrix of an invariant factor of  $A$ .

**Derivation:**

- Let  $k[x] \curvearrowright V$  using  $T$ , take invariant factors  $a_i$ ,
- Note that  $T \curvearrowright V$  by multiplication by  $x$
- Write  $\bar{x} = \pi(x)$  where  $F[x] \xrightarrow{\pi} F[x]/(a_i)$ ; then  $\text{span}\{\bar{x}\} = F[x]/(a_i)$ .
- Write  $a_i(x) = \sum b_i x^i$ , note that  $V \rightarrow F[x]$  pushes  $T \curvearrowright V$  to  $T \curvearrowright k[x]$  by multiplication by  $\bar{x}$
- WRT the basis  $\bar{x}$ ,  $T$  then acts via the companion matrix on this summand.
- Each invariant factor corresponds to a block of the RCF.

#### 4.4.2 Jordan Canonical Form

Corresponds to the **Elementary Divisor Decomposition** of  $T$ .

**Lemma:** The elementary divisors of  $A$  are the minimal polynomials of the Jordan blocks.

**Lemma:** Writing

$$\begin{aligned}\min_A(x) &= \prod (x - \lambda_i)^{a_i} \\ \chi_A(x) &= \prod (x - \lambda_i)^{b_i}\end{aligned}$$

- $a_i \leq b_i$
- $a_i$  tells you the size of the **largest** Jordan block associated to  $\lambda_i$ ,
- $b_i$  is the **sum of sizes** of all Jordan blocks associated to  $\lambda_i$
- $\dim E_{\lambda_i}$  is the **number of Jordan blocks** associated to  $\lambda_i$

#### 4.5 Using Canonical Forms

**Lemma:** The characteristic polynomial is the *product of the invariant factors*, i.e.

$$\chi_A(x) = \prod_{j=1}^n f_j(x).$$

**Lemma:** The minimal polynomial of  $A$  is the *invariant factor of highest degree*, i.e.

$$\min_A(x) = f_n(x).$$

**Lemma:** For a linear operator on a vector space of nonzero finite dimension, TFAE:

- The minimal polynomial is equal to the characteristic polynomial.
- The list of invariant factors has length one.
- The Rational Canonical Form has a single block.

- The operator has a matrix similar to a companion matrix.
- There exists a *cyclic vector*  $\mathbf{v}$  such that  $\text{span}_k \{T^j \mathbf{v} \mid j = 1, 2, \dots\} = V$ .
- $T$  has  $\dim V$  distinct eigenvalues

## 4.6 Diagonalizability

*Notation:*  $A^*$  denotes the conjugate transpose of  $A$ .

**Lemma:** Let  $V$  be a vector space over  $k$  an algebraically closed and  $A \in \text{End}(V)$ . Then if  $W \subseteq V$  is an invariant subspace, so  $A(W) \subseteq W$ , the  $A$  has an eigenvector in  $W$ .

**Theorem (The Spectral Theorem):**

1. Hermitian matrices (i.e.  $A^* = A$ ) are diagonalizable over  $\mathbb{C}$ .
2. Symmetric matrices (i.e.  $A^t = A$ ) are diagonalizable over  $\mathbb{R}$ .

*Proof:* Suppose  $A$  is Hermitian. Since  $V$  itself is an invariant subspace,  $A$  has an eigenvector  $\mathbf{v}_1 \in V$ . Let  $W_1 = \text{span}_k \{\mathbf{v}_1\}^\perp$ . Then for any  $\mathbf{w}_1 \in W_1$ ,

$$\langle \mathbf{v}_1, A\mathbf{w}_1 \rangle = \langle A\mathbf{v}_1, \mathbf{w}_1 \rangle = \lambda \langle \mathbf{v}_1, \mathbf{w}_1 \rangle = 0,$$

so  $A(W_1) \subseteq W_1$  is an invariant subspace, etc.

Suppose now that  $A$  is symmetric. Then there is an eigenvector of norm 1,  $\mathbf{v} \in V$ .

$$\lambda = \lambda \langle \mathbf{v}, \mathbf{v} \rangle = \langle A\mathbf{v}, \mathbf{v} \rangle = \langle \mathbf{v}, A\mathbf{v} \rangle = \bar{\lambda} \implies \lambda \in \mathbb{R}.$$

**Lemma:**  $\{A_i\}$  pairwise commute  $\iff$  they are all simultaneously diagonalizable.

*Proof:* By induction on number of operators

- $A_n$  is diagonalizable, so  $V = \bigoplus E_i$  a sum of eigenspaces
- Restrict all  $n - 1$  operators  $A$  to  $E_n$ .
- The commute in  $V$  so they commute in  $E_n$
- **(Lemma)** They were diagonalizable in  $V$ , so they're diagonalizable in  $E_n$
- So they're simultaneously diagonalizable by I.H.
- But these eigenvectors for the  $A_i$  are all in  $E_n$ , so they're eigenvectors for  $A_n$  too.
- Can do this for each eigenspace. ■

Full details here

**Theorem (Characterizations of Diagonalizability)**

$M$  is diagonalizable over  $\mathbb{F} \iff \min_M(x, \mathbb{F})$  splits into distinct linear factors over  $\mathbb{F}$ , or equivalently iff all of the roots of  $\min_M$  lie in  $\mathbb{F}$ .

*Proof:*  $\implies$  : If  $\min_A$  factors into linear factors, so does each invariant factor, so every elementary divisor is linear and  $JCF(A)$  is diagonal.

$\impliedby$  : If  $A$  is diagonalizable, every elementary divisor is linear, so every invariant factor factors into linear pieces. But the minimal polynomial is just the largest invariant factor.

## 4.7 Matrix Counterexamples

1. A matrix that is:

- Not diagonalizable over  $\mathbb{R}$  but diagonalizable over  $\mathbb{C}$
- No eigenvalues in  $\mathbb{R}$  but distinct eigenvalues over  $\mathbb{C}$
- $\min_M(x) = \chi_M(x) = x^2 + 1$

$$M = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \sim \left[ \begin{array}{c|c} -1\sqrt{-1} & 0 \\ \hline 0 & 1\sqrt{-1} \end{array} \right].$$

2.

$$M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

- Not diagonalizable over  $\mathbb{C}$
  - Eigenvalues  $[1, 1]$  (repeated, multiplicity 2)
  - $\min_M(x) = \chi_M(x) = x^2 - 2x + 1$
3. Non-similar matrices with the same characteristic polynomial

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

4. A full-rank matrix that is not diagonalizable:

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

5. Matrix roots of unity:

$$\sqrt{I_2} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

$$\sqrt{-I_2} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

## 4.8 Miscellaneous

**Lemma:**  $I \trianglelefteq R$  is a free  $R$ -module iff  $I$  is a principal ideal.



Proof:  $\implies$  :

Suppose  $I$  is free as an  $R$ -module, and let  $B = \{\mathbf{m}_j\}_{j \in J} \subseteq I$  be a basis so we can write  $M = \langle B \rangle$ .

Suppose that  $|B| \geq 2$ , so we can pick at least 2 basis elements  $\mathbf{m}_1 \neq \mathbf{m}_2$ , and consider

$$\mathbf{c} = \mathbf{m}_1\mathbf{m}_2 - \mathbf{m}_2\mathbf{m}_1,$$

which is also an element of  $M$ .

Since  $R$  is an integral domain,  $R$  is commutative, and so

$$\mathbf{c} = \mathbf{m}_1\mathbf{m}_2 - \mathbf{m}_2\mathbf{m}_1 = \mathbf{m}_1\mathbf{m}_2 - \mathbf{m}_1\mathbf{m}_2 = \mathbf{0}_M$$

However, this exhibits a linear dependence between  $\mathbf{m}_1$  and  $\mathbf{m}_2$ , namely that there exist  $\alpha_1, \alpha_2 \neq 0_R$  such that  $\alpha_1\mathbf{m}_1 + \alpha_2\mathbf{m}_2 = \mathbf{0}_M$ ; this follows because  $M \subset R$  means that we can take  $\alpha_1 = -m_2, \alpha_2 = m_1$ . This contradicts the assumption that  $B$  was a basis, so we must have  $|B| = 1$  and so  $B = \{\mathbf{m}\}$  for some  $\mathbf{m} \in I$ . But then  $M = \langle B \rangle = \langle \mathbf{m} \rangle$  is generated by a single element, so  $M$  is principal.

$\Leftarrow$  :

Suppose  $M \trianglelefteq R$  is principal, so  $M = \langle \mathbf{m} \rangle$  for some  $\mathbf{m} \neq \mathbf{0}_M \in M \subset R$ .

Then  $x \in M \implies x = \alpha\mathbf{m}$  for some element  $\alpha \in R$  and we just need to show that  $\alpha\mathbf{m} = \mathbf{0}_M \implies \alpha = 0_R$  in order for  $\{\mathbf{m}\}$  to be a basis for  $M$ , making  $M$  a free  $R$ -module.

But since  $M \subset R$ , we have  $\alpha, m \in R$  and  $\mathbf{0}_M = 0_R$ , and since  $R$  is an integral domain, we have  $\alpha m = 0_R \implies \alpha = 0_R$  or  $m = 0_R$ .

Since  $m \neq 0_R$ , this forces  $\alpha = 0_R$ , which allows  $\{\mathbf{m}\}$  to be a linearly independent set and thus a basis for  $M$  as an  $R$ -module. ■