Algebra Notes

D. Zack Garza

January 6, 2020

Contents

1 Group Theory

Definition (Centralizer):

$$C_G(H) = \left\{ g \in G \;\middle|\; ghg^{-1} = h \; \forall h \in H \right\}$$

Definition (Normalizer):

$$N_G(H) = \left\{ g \in G \;\middle|\; gHg^{-1} = H \right\}$$

Lemma: $C_G(H) \leq N_G(H)$

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

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

Lemma ("The Fundamental Theorem of Cosets"):

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

Definition: $[x, y] = x^{-1}y^{-1}xy$ is the **commutator**, and $[G, G] \coloneqq \left\{ [x, y] \;\middle|\; x, y \in G \right\}$ is the **commutator subgroup**.

Lemma:

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

1.1 Finitely Generated Abelian Groups

Invariant factor decomposition:

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

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

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

1.2 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. $A_n \coloneqq \left\{\sigma \in S_n \;\middle|\; \operatorname{sign}(\sigma) = 1\right\}$ where $\operatorname{sign}(\sigma) = (-1)^m$ 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:

$$\begin{aligned}A_4 = \{&\mathrm{id},\\ &(1,3)(2,4),(1,2)(3,4),(1,4)(2,3),\\ &(1,2,3),(1,3,2),\\ &(1,2,4),(1,4,2),\\ &(1,3,4),(1,4,3),\\ &(2,3,4),(2,4,3)\}.\end{aligned}$$

Lemmas:

- The transitive subgroups of S_3 are S_3, A_3
- The transitive subgroups of S_4 are $S_4, A_4, D_4, \mathbb{Z}_2^2, \mathbb{Z}_4$.
- For $n = 4, S_n$ has two normal subgroups: $A_4, \mathbb{Z}_2^2$.
- For $n \geq 5, S_n$ 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 $n \geq 5$
- A_n is *simple* for $n \geq 5$.

1.3 Counting Theorems

Lagrange's Theorem:

$$H \leq G \implies |H| \,\Big|\, |G|.$$

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

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

Warning: Rhere does **not** necessarily exist $H \leq G$ with $|H| = n$ for every $n \,\Big|\, |G|$.
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.

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

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

- $X^g = \left\{ x \in X \;\middle|\; g \curvearrowright x = x \right\} \subseteq X$ are the fixed points

Orbit-Stabilizer:

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

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

1.3.1 Examples of Orbit-Stabilizer

1. Let G act on itself by conjugation.

- $G \cdot x$ is the **conjugacy class** of x
- $G_x = Z(x) \coloneqq C_G(x) = \left\{ g \;\middle|\; [g, x] = e \right\}$, the **centralizer** of x.
- G^g (the fixed points) is the **center** $Z(G)$.

Corollary: The size of a conjugacy class is the index of the centralizer.
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.

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

3. For a fixed proper subgroup $H < G$, let G act on its cosets $G/H = \left\{ gH \;\middle|\; g \in G \right\}$ 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 ϕ; it is nontrivial since $gH = H$ for all g implies $H = G$; $\ker \phi \trianglelefteq G$ and G simple implies $\ker \phi = 1$.

Burnside's Formula:

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

1.3.2 Sylow Theorems

Notation: For any p, let $\mathrm{Syl}_p(G)$ 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 $\mathbb{Z}_p, \mathbb{Z}_q \subset G \implies \mathbb{Z}_p \bigcap \mathbb{Z}_q = \mathbb{Z}_{(p,q)}$.
- The Chinese Remainder theorem: $(p, q) = 1 \implies \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$

1.3.3 Sylow 1 (Cauchy for Prime Powers)

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

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.

1.3.4 Sylow 2 (Sylows are Conjugate)

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

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

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

1.3.5 Sylow 3 (Numerical Constraints)

1. $n_p \mid m$ (in particular, $n_p \leq m$),
2. $n_p \equiv 1 \mod p$,
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 $H \subsetneq H^1 \subsetneq \cdots$, 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 $P \in \mathrm{Syl}_p(G)$, then $HN_G(P) = G$ and $[G : H]$ divides $|N_G(P)|$.

1.4 Products

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

- $G = HK = \left\{hk \,\middle|\, h \in H, k \in K\right\}$
- $H \bigcap K = \{e\} \subset G$
- $H, K \trianglelefteq G$

> 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

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

> *Lemma:* If $\sigma \in \mathrm{Aut}(H)$, then $N \rtimes_\psi H \cong N \rtimes_{\psi \circ \sigma} H$.

Useful Facts

- $\mathrm{Aut}(\prod_{k=1}^n \mathbb{Z}/(p)) = \mathrm{GL}(n, \mathbb{Z}/(p))$
  - If this occurs in a semidirect product, it suffices to consider similarity classes of matrices (i.e. just use canonical forms)
- $\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}^n)^\times \cong \mathbb{Z}^{\varphi(n)}$ where φ is the totient function.

1.5 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.

Diamond Theorem / 2nd Isomorphism Theorem:

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

$$\frac{SN}{N} \cong \frac{S}{S \bigcap N}$$

> Note: for this to make sense, we also have
>
> - $SN \leq G$,
> - $S \bigcap N \trianglelefteq S$,

Cancellation / 3rd Isomorphism Theorem

Figure 1: Image

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

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

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

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

$$\begin{aligned} \left\{H < G \;\middle|\; N \subseteq H\right\} &\iff \left\{H \;\middle|\; H < \frac{G}{N}\right\} \\ \{\} &\iff \{\}\,. \end{aligned}$$

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: $N \trianglelefteq G$ and $N \subseteq H < G \implies N \trianglelefteq H$.

1.6 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 $N \trianglelefteq G$.

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

Lemmas:

- p-groups have nontrivial centers

- 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*

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 $N \to E \to G/N$. >

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

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

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

1.7 Series of Groups

Definition: A **normal series** of a group G is a sequence $G \to G^1 \to G^2 \to \cdots$ 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-Holder): Any two composition series of a group have the same length and isomorphic factors (up to permutation).1

Definition A **derived series** of a group G is a normal series $G \to G^1 \to G^2 \to \cdots$ 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 $G \to G^1 \to \cdots \to \{e\}$ 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 $G \to G^1 \to \cdots \to \{e\}$ 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 $G \to G^1 \to \cdots \to \{e\}$ 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 and Basics

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

Definition: $\mathrm{Spec}(R) = \left\{ \mathfrak{p} \trianglelefteq R \;\middle|\; \mathfrak{p} \text{ is prime} \right\}$ is the **spectrum** of R.

Definition: $\mathfrak{m}$ is **maximal** $\iff I \trianglelefteq R \implies I \subseteq \mathfrak{m}$.

Definition: $\mathrm{Spec}_{\max}(R) = \left\{ \mathfrak{m} \trianglelefteq R \;\middle|\; \mathfrak{m} \text{ is maximal} \right\}$ is the **max-spectrum** of R.

> Note: nonstandard notation / definition.

Lemma: Field $\implies$ Euclidean Domain $\implies$ PID $\implies$ UFD $\implies$ Integral Domain.

2.2 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 Nilradical and Jacobson Radical

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

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

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

Proof:
$\mathfrak{N} \subseteq \bigcap \mathfrak{p}$: $x \in \mathfrak{N} \implies x^n = 0 \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $x^{n-1} \in \mathfrak{p}$.
$\mathfrak{N}^c \subseteq \bigcup \mathfrak{p}^c$: Define $S = \left\{ I \trianglelefteq R \;\middle|\; a^n \notin I \text{ for any } n \right\}$. 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.

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

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.

2.4 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.

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

Lemma: If $I_1 \subseteq I_2 \subseteq \cdots$ 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
>
> $$S = \left\{ J \;\middle|\; I \subseteq J < R \right\}.$$
>
> 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 $C = \{C_1 \subseteq C_2 \subseteq \cdots\}$ 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.
>
> ■

2.5 Unsorted

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 ϕ 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.

3 Fields

Lemma: Let $\phi_n := x^{p^n} - x$. Then $f(x) \;\middle|\; \phi_n(x) \iff \deg f \;\middle|\; n$ and f is irreducible.

(So $\phi_n = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n.)

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

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

3.1 Cyclotomic Polynomials

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

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

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

Computing Φ_n:

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

   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:

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

Theorem: $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/(n)^\times$ and is generated by maps of the form $\zeta_n \mapsto \zeta_n^j$ where $(j, n) = 1$.

3.2 Finite Fields

Theorem: $\mathbb{GF}(p^n)$ is obtained as $\dfrac{\mathbb{F}_p}{\langle f \rangle}$ where $f \in \mathbb{F}_p[x]$ is irreducible of degree n.

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

- $p \not\Big| a_n$ but $p \Big| a_{i \neq n}$, and
- $p^2 \not\Big| a_0$,

then f is irreducible.

3.3 Galois Theory

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

Definition: A field extension L/k is **normal** iff

- Every embedding $\sigma : L \hookrightarrow \overline{k}$ that is a lift of the identity over k satisfies $\sigma(L) = L$.
- Every irreducible $f \in k[x]$ that has one root in L has all of its roots in L
- If L is separable: L is the splitting field of some irreducible $f \in k[x]$.

Definition: A field extension L/k is **separable** iff

- For every $\alpha \in L, f(x) \coloneqq \min(\alpha, k)$ equivalently has
  - No repeated factors/roots
  - $f' \not\equiv 0$, or
  - $\gcd(f, f') = 1$.

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

Definition: Let L/k be a finite field extension. TFAE:

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

Lemmas about towers: Let $L/F/k$ be a tower of field extensions

- L/k normal $\implies L/F$ normal.
- L/k Galois $\implies L/F$ Galois.
- F/k is Galois $\iff \mathrm{Gal}(L/F) \trianglelefteq \mathrm{Gal}(L/k)$
  - $\implies \mathrm{Gal}(F/k) \cong \dfrac{\mathrm{Gal}(L/k)}{\mathrm{Gal}(L/F)}$
- **Every** quadratic extension is Galois.

4 Modules

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

$\implies$:

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.

$\impliedby$:

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 $\{m\}$ to be a linearly independent set and thus a basis for M as an R-module.

■

5 Linear Algebra

5.1 Minimal / Characteristic Polynomial

Finding the minimal polynomial $m(x)$ of 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 $T\mathbf{v}, T^2\mathbf{v}, \cdots T^k\mathbf{v}$ until a linear dependence is introduced. Write this as $p(T) = 0$; then $\chi(x)\ p(x)$.

5.2 Simultaneous Diagonalizability

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 commuted 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

5.3 Characterizations if Diagonalizability

Let $\min_M(x)$ denote the minimal polynomial of A and $\chi_M(x)$ the characteristic polynomial.

Lemma:

$$\chi_M(x) = \prod_{i=1}^{k} (x-\lambda_i)^{m_i} \implies \min_M(x) = \prod_{i=1}^{k} (x-\lambda_i)^{\ell_i} \text{ where } 1 \leq \ell_i \leq m_i,$$

where λ_i are eigenvalues of M, m_i is the multiplicity of λ_i.

Proof: Since $\mathbb{C}$ is algebraically closed, p_M splits into linear factors where $\sum m_i = n$. By Cayley-Hamilton, p_M annihilates M, and so by definition, μ_M divides p_M. Finally, every λ_i is a root of μ_M: let $\mathbf{v}_i$ be the eigenvector associated to λ_i, so $\mathbf{v}_i \neq \mathbf{0}$ and $M\mathbf{v}_i = \lambda_i \mathbf{v}_i$. Then by linearity $\mu_M(\lambda_i)\mathbf{v}_i = \mu_M(M)\mathbf{v}_i = \mathbf{0}$, which forces $\mu_M(\lambda_i) = 0$.

Lemma:

$$M \text{ is diagonalizable over } \mathbb{F} \iff \min_M(x) \text{ splits into distinct linear factors over } \mathbb{F}.$$

(Equivalently, iff all of the roots of $\min_M$ lie in $\mathbb{F}$)

Proof:
$\implies$:
If M is diagonalizable, its domain has a basis of eigenvectors. So if $\mathbf{x} \in \text{domain}(M), \mathbf{v} = \sum \alpha_i \mathbf{v}_i$ where $\mathbf{v}_i$ are eigenvectors. Then $q(x) = \prod_{i=1}^{k} (x - \lambda_i)$ annihilates M, because we have

$$q(M)\mathbf{w} = q(M) \sum_i \alpha_i \mathbf{v}_i = \sum_i \alpha_i \prod_j (M - I\lambda_j)\mathbf{v}_i = \mathbf{0}$$

where the last equality follows because $(M - I\lambda_i)\mathbf{v}_i = \mathbf{0}$ and for each i, a factor of $(M - I\lambda_i)$ in the product will annihilate $\mathbf{v}_i$. By minimality, μ_M must divide q, but we must have $k \leq \deg \mu_M \leq n$, so this forces $\deg \mu_M = k$. But then we have two monic polynomials of degree k with the same roots, forcing them to be identical.
$\impliedby$: Longer proof, omitted.

5.4 Canonical Forms

Fix $T : V \to V$, and decompositions

$$V = \bigoplus_{j=1}^{n} \frac{k[x]}{(f_j)} \quad \text{(invariant factors)}.$$

Fix some notation:

$$\begin{aligned} \chi_T(x) &: \quad \text{The characteristic polynomial of } A \\ \min_T(x) &: \quad \text{The minimal polynomial of } A. \end{aligned}$$

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

5.4.1 Rational Canonical Form

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

Derivation:

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

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* v such that $\operatorname{span}_k \left\{ T^j \mathbf{v} \;\middle|\; j = 1, 2, \cdots \right\} = V$.
- T has $\dim V$ distinct eigenvalues

5.4.2 Jordan Canonical Form

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

Derivation Todo

Facts:

- The following can be read directly off of the invariant factor decomposition:
  - The minimal polynomial is the *invariant factor of highest degree*, i.e.
$$\min_T(x) = f_n(x).$$
  - The characteristic polynomial is the *product of the invariant factors*, i.e.
$$\chi_T(x) = \prod_{j=1}^n f_j(x).$$
- Both $\min_T(x)$ and $\chi_T(x)$ have roots precisely the eigenvalues of T, with potentially different multiplicities.
- Writing
$$\begin{aligned} \min_A(x) &= \prod (x-\lambda_i)^{a_i} \\ \chi_A(x) &= \prod (x-\lambda_i)^{b_i} \end{aligned}$$
  then $a_i \leq b_i$, and
  - a_i tells you the size of the **largest** Jordan block associated to λ_i,
  - b_i is the **sum of sizes** of all Jordan blocks associated to λ_i
  - $\dim E_{\lambda_i}$ is the **number of Jordan blocks** associated to λ_i
- The elementary divisors of A are the minimal polynomials of the Jordan blocks.
- For characteristic polynomials
$$p(x) = \det(A - x1)) = \det(SNF(A - x1)).$$
- ? Invariant factors of A are the invariant factors of $xI
- A$ over $k[x]$, and $\prod a_i = \det(xI - A)$.

5.5 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 $\mathbb{C}$
- $\min_M(x) = \chi_M(x) = x^2 + 1$

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

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:

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

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