Algebra Qualifying Exam Review

D. Zack Garza

Saturday 25^{th} July, 2020

Contents

1 Topics and Remarks 2

Adapted from remark written by Roy Smith, August 2006

> "As a general rule, students are responsible for knowing both the theory (proofs) and practical applications (e.g. **how to find the Jordan or rational canonical form** of a given matrix, **or the Galois group of a given polynomial**) of the topics mentioned."

1.1 References

- [1] David Dummit and Richard Foote, Abstract Algebra, Wiley, 2003.
- [2] Kenneth Hoffman and Ray Kunze, Linear Algebra, Prentice-Hall, 1971.
- [3] Thomas W. Hungerford, Algebra, Springer, 1974.
- [4] Roy Smith, Algebra Course Notes (843-1 through 845-3), `http://www.math.uga.edu/~roy/`,

1.2 Group Theory

References: [1], [3], [4]

> "The first 6 chapters (220 pages) of Dummit and Foote are excellent. All the definitions and proofs of these theorems on groups are given in Smith's web based lecture notes for math 843 part 1."

Key Topics:

- Sylow theorems
- Simplicity of A_n for $n > 4$.
- The first isomorphism theorem,
- The Jordan Holder theorem,

  > The last two (one easy, one hard) are left as exercises.

  The proof of Jordan-Holder is seldom tested on the qual, but proofs are always of interest.
- Fundamental theorem of finite abelian groups

  DF Exercises 12.1.16-19
- The simple groups of order between 60 and 168 have prime order

Full List of Topics

- Chapters 1-9 of Dummit and Foote
- Subgroups and quotient groups
- Lagrange's Theorem
- Fundamental homomorphism theorems
- Group actions with applications to the structure of groups such as
  - The Sylow Theorems
- Group constructions such as:

  - Direct and semi-direct products
- Structures of special types of groups such as:
  - p-groups
  - Dihedral,
  - Symmetric and Alternating groups
    * Cycle decompositions
- The simplicity of A_n, for $n \geq 5$
- Free groups, generators and relations
- Solvable groups
- Left and right cosets
- Lagrange's theorem
- Isomorphism theorems
- Group generated by a subset
- Structure of cyclic groups
- Composite groups
- Normalizer
- Symmetric groups
- Cayley's theorem
- Orbit stabilizer theorem
- Orbits act on left cosets of subgroups
- Subgroups of index p, the smallest prime dividing $|G|$, are normal
- Action of G on itself by conjugation
- Class equation
- p-groups
- p^2 groups are abelian
- Automorphisms
  - Inner automorphisms
- Proof of Sylow theorems
- A_n is simple for $n \geq 5$
- Recognition of internal direct product
- Recognition of semi-direct product
- Classification of groups of order pq
- Free group & presentations

- Commutator subgroup
- Solvable groups
- Derived series
- Nilpotent groups
- Upper central series
- Lower central series
- Fratini's argument

1.3 Linear Algebra

References: [1],[2],[4]

- Determinants
- Eigenvalues and eigenvectors
- Cayley-Hamilton Theorem
- Canonical forms for matrices
- Linear groups ($\mathrm{GL}_n, \mathrm{SL}_n, \mathrm{O}_n, \mathrm{U}_n$)
- Duality
  - Dual spaces,
  - Dual bases,
  - Induced dual map,
  - Double duals
- Finite-dimensional spectral theorem

1.4 Rings

References: [1],[3],[4]

- DF chapters 13,14 (about 145 pages).
- Smith:
  - 843-2, sections 11,12, and 16-21 (39 pages)
  - 844-1, sections 7-9 (20 pages)
  - 844-2, sections 10-16, (37 pages)

Full List of Topics:

- Properties of ideals and quotient rings
- I maximal iff R/I is a field
- Zorn's lemma
  - Every vector space has a basis

  - Maximal ideals exist

- Chinese Remainder Theorem
- Localization of a domain
- Field of fractions
- Factorization in domains
- Euclidean algorithm
- Gaussian integers
- Primes and irreducibles
- Characterizations and properties of special rings such as:
  - Euclidean $\implies$ PID $\implies$ UFD
  - Domains
    * Primes are irreducible
  - UFDs
    * Have GCDs
    * Sometimes PIDs
  - PIDs
    * Noetherian
    * Irreducibles are prime
    * Are UFDs
    * Have GCDs
  - Euclidean domains
    * Are PIDs
- Factorization in $Z[i]$
- Polynomial rings
- Gauss' lemma
- Remainder and factor theorem
- Polynomials
- Reducibility
- Rational root test
- Eisenstein's criterion
- DF Chapters 7, 8, 9.
- Gauss's important theorem on unique factorization of polynomials:
  - $\mathbb{Z}[x]$ is a UFD
  - $R[x]$ is a UFD when R is a UFD
- The fundamental isomorphism theorems for rings

  An easy and useful exercise

- How to use Zorn's lemma
  - To find maximal ideals
  - Construct algebraic field closures
  - Why it is unnecessary in countable or noetherian rings.

  Smith discusses extensively in 844-1.

- Results about PIDs *(DF Section 8.2)*
  - Example of a PID that is not a Euclidean domain *(DF p.277)*
  - Proof that a Euclidean domain is a PID and hence a UFD
  - Proof that $\mathbb{Z}$ and $k[x]$ are UFDs *(p.289 Smith, p.300 DF)*
- A polynomial ring in infinitely many variables over a UFD is still a UFD *(Easy, DF, p.305)*
- Eisenstein's criterion *(DF p.309)*

  Stated only for monic polynomials – proof of general case identical. See Smith's notes for the full version.

- Cyclic product structure of $(\mathbb{Z}/n\mathbb{Z})^\times$

  Exercise in DF, Smith 844-2, section 18

- Gröbner bases and division algorithms for polynomials in several variables *(DF 9.6.)*

1.5 Modules

References: [1],[3],[4]

- Fundamental homomorphism theorems for rings and modules
- Applications to the structure of:
  - Finitely generated abelian groups
  - Canonical forms of matrices
- Classification of finitely generated modules over PIDs *(with emphasis on Euclidean Domains)*
- Modules over PIDs and canonical forms of matrices.

  DF sections 10.1, 10.2, 10.3, and 12.1, 12.2, 12.3.

  - Constructive proof of decomposition: DF Exercises 12.1.16-19
  - Smith 845-1 and 845-2: Detailed discussion of the constructive proof.

1.6 Field Theory

References: [1],[3],[4]

- Algebraic extensions of fields
- Properties of finite fields
- Separable extensions

- Fundamental theorem of Galois theory
- Computations of Galois groups of polynomials of small degree and cyclotomic
- Polynomials
- Solvability of polynomials by radicals

2 Group Theory

- 2^X denotes the powerset of X.
- For any p dividing the order of G, $\mathrm{Syl}_p(G)$ denotes the *set* of Sylow-p subgroups of G.

2.1 Big List of Notation

$C_G(x) =$	$\left\{g \in G \,\middle\vert\, [g,x] = 1\right\}$	$\subseteq G$	Centralizer (Element)
$C_G(H) =$	$\left\{g \in G \,\middle\vert\, [g,h] = 1 \;\forall h \in H\right\} = \bigcap_{h \in H} C_G(h)$	$\leq G$	Centralizer (Subgroup)
$C(h) =$	$\left\{ghg^{-1} \,\middle\vert\, g \in G\right\}$	$\subseteq G$	Conjugacy Class
$Z(G) =$	$\left\{x \in G \,\middle\vert\, \forall g \in G,\; gxg^{-1} = x\right\}$	$\subseteq G$	Center
$N_G(H) =$	$\left\{g \in G \,\middle\vert\, gHg^{-1} = H\right\}$	$\subseteq G$	Normalizer
$\mathrm{Inn}(G) =$	$\left\{\varphi_g(x) = gxg^{-1}\right\}$	$\subseteq \mathrm{Aut}(G)$	Inner Aut.
$\mathrm{Out}(G) =$	$\mathrm{Aut}(G)/\mathrm{Inn}(G)$	$\hookrightarrow \mathrm{Aut}(G)$	Outer Aut.
$[g,h] =$	$ghgh^{-1}$	$\in G$	Commutator (Element)
$[G,H] =$	$\left\langle \left\{[g,h] \,\middle\vert\, g \in G, h \in H\right\} \right\rangle$	$\leq G$	Commutator (Subgroup)
$\mathcal{O}_x$ or $G \cdot x =$	$\left\{g.x \,\middle\vert\, x \in X\right\}$	$\subseteq X$	Orbit
$\mathrm{Stab}_G(x)$ or $G_x =$	$\left\{g \in G \,\middle\vert\, g.x = x\right\}$	$\subseteq G$	Stabilizer
$X/G =$	$\left\{G_x \,\middle\vert\, x \in X\right\}$	$\subseteq 2^X$	Set of Orbits
$X^g =$	$\left\{x \in X \,\middle\vert\, \forall g \in G,\; g.x = x\right\}$	$\subseteq X$	Fixed Points

Definition 2.0.1 (Normal Closure of a Subgroup)**.**
The smallest normal subgroup of G containing H:

$$H^G \coloneqq \{gHg^{-1} : g \in G\} = \bigcap \{N : H \leq N \trianglelefteq G\}\,.$$

Definition 2.0.2 (Normal Core of a subgroup)**.**
The largest normal subgroup of G containing H:

$$H_G = \bigcap_{g \in G} gHg^{-1} = \langle N : N \trianglelefteq G \ \&\ N \leq H \rangle = \ker \psi.$$

where

$$\begin{aligned} \psi : G &\longrightarrow \mathrm{Aut}(G/H) \\ g &\mapsto (xH \mapsto gxH) \end{aligned}$$

Definition 2.0.3 (Characteristic subgroup)**.**
$H \leq G$ is *characteristic* iff H is fixed by every element of $\mathrm{Aut}(G)$.

Definition 2.0.4 (Subgroup Generated by a Subset)**.**
If $H \subset G$, then $\langle H \rangle$ is the smallest subgroup containing H:

$$\langle H \rangle = \bigcap \left\{ H \;\middle|\; H \subseteq M \leq G \right\} M = \left\{ h_1^{\pm 1} \cdots h_n^{\pm 1} \;\middle|\; n \geq 0, h_i \in H \right\}$$

Definition 2.0.5 (Centralizer)**.**

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

Definition 2.0.6 (Normalizer)**.**

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

Theorem 2.1 ***(The Fundamental Theorem of Cosets).***
$aH = bH \iff a^{-1}b \in H$ or $aH \bigcap bH = \emptyset$

Definition 2.1.1 (The Quaternion Group)**.**
The *Quaternion group* of order 8 is given by

$$\begin{aligned} Q &= \left\langle x, y, z \;\middle|\; x^2 = y^2 = z^2 = xyz = -1 \right\rangle \\ &= \left\langle x, y \;\middle|\; x^4 = y^4, x^2 = y^2, yxy^{-1} = x^{-1} \right\rangle \end{aligned}$$

Definition 2.1.2 (The Dihedral Group)**.**
A *dihedral group* of order $2n$ is given by

$$D_n = \left\langle r, s \;\middle|\; r^n, s^2, rsr^{-1} = s^{-1} \right\rangle$$

2.2 The Symmetric Group

Definition 2.1.3 (Parity of a Cycle)**.**
- 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**

Mnemonic: the parity of a k-cycle is the parity of $k-1$.

Definition 2.1.4 (Alternating Group)**.**
The **alternating group** is the subgroup of **even** permutations, i.e.

$$A_n := \left\{ \sigma \in S_n \;\middle|\; \operatorname{sign}(\sigma) = 1 \right\}$$

where $\operatorname{sign}(\sigma) = (-1)^m$ and m is the number of cycles of even length.

Corollary 2.2*(Alternating Group).*
Every $\sigma \in A_n$ has an even number of *odd* cycles (i.e. an even number of *even-length* cycles).

Example 2.1.

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

Definition 2.2.1 (Transitive Subgroup)**.**
A subgroup of S_n is **transitive** iff its action on $\{1, 2, \cdots, n\}$ is transitive.

Useful Facts:

- $\sigma \circ (a_1 \cdots a_k) \circ \sigma^{-1} = (\sigma(a_1), \cdots \sigma(a_k))$
- Conjugacy classes are determined by cycle type
- The order of a cycle is its length.
- The order of an element is the least common multiple of the sizes of its cycles.
- $A_{n\geq 5}$ is *simple*.

2.3 Counting Theorems

Theorem 2.3 ***(Lagrange's Theorem).***

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

Corollary 2.4.
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:** There 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.

Theorem 2.5 ***(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.

2.3.1 Group Actions

Definition 2.5.1 (Group Action)**.**
An action of G on X is a group morphism

$$\begin{aligned}\varphi : G \times X &\to X \\ (g, x) &\mapsto g \cdot x\end{aligned}$$

or equivalently

$$\begin{aligned}\varphi : G &\longrightarrow \operatorname{Aut}(X) \\ g \mapsto (x \mapsto \varphi_g(x) &\coloneqq g \cdot x)\end{aligned}$$

satisfying

1. $e \cdot x = x$
2. $g \cdot (h \cdot x) = (gh) \cdot x$

Useful fact: $\ker \psi = \displaystyle\bigcap_{x \in X} G_x$ is the intersection of all stabilizers.

Definition 2.5.2 (Transitive Group Action)**.**
A group action $G \curvearrowright X$ is *transitive* iff for all $x, y \in X$ there exists a $g \in G$ such that $g \cdot x = x$. Equivalently, the action has a single orbit.

Reminder of notation: for a group G acting on a set X,

- $G \cdot x = \left\{ g \cdot x \;\middle|\; g \in G \right\} \subseteq X$ is the orbit
- $G_x = \left\{ g \in G \;\middle|\; g \cdot x = x \right\} \subseteq G$ is the stabilizer
- $X/G \subset 2^X$ is the set of orbits
- $X^g = \left\{ x \in X \;\middle|\; g \cdot x = x \right\} \subseteq X$ are the fixed points

Note that being in the same orbit is an equivalence relation which partitions X, and G acts transitively if restricted to any single orbit.

Theorem 2.6 ***(Orbit-Stabilizer).***

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

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

2.3.2 Examples of Orbit-Stabilizer

1. Let G act on itself by left translation, where $g \mapsto (h \mapsto gh)$.

- The orbit $G \cdot x = G$ is the entire group
- The stabilizer G_x is only the identity.
- The fixed points X^g are only the identity.

2. Let G act on *itself* by conjugation.

- $G \cdot x$ is the **conjugacy class** of x (so not generally transitive)
- $G_x = Z(x) \coloneqq C_G(x) = \left\{ g \;\middle|\; [g, x] = e \right\}$, the **centralizer** of x.
- G^g (the fixed points) is the **center** $Z(G)$.

Corollary 2.7.
The number of conjugates of an element (i.e. the size of its conjugacy class) is the index of its centralizer, $[G : C_G(x)]$.

2.3.3 The Class Equation

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

Note that $[G : C_G(x_i)]$ is the number of elements in the conjugacy class of x_i, and each $x_i \in Z(G)$ has a singleton conjugacy class.

Examples

1. Let G act on X, 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
- X^g is the set of **normal subgroups** of G

Corollary 2.8.
Given $H \leq G$, the number of conjugate subgroups is $[G : N_G(H)]$.

2. For a fixed proper subgroup $H < G$, let G act on its cosets $G/H = \left\{gH \;\middle|\; g \in G\right\}$ by left translation.

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

Proposition 2.9 ***(Application of the Class Equation).***
If G is simple, $H < G$ proper, and $[G : H] = n$, then there exists an injective map $\varphi : G \hookrightarrow S_n$.

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

■

Theorem 2.10 ***(Burnside's Formula).***
Slogan: the number of orbits is equal to the average number of fixed points, i.e.

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

2.3.4 Sylow Theorems

Definition 2.10.1.
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.

Write

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

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: $(p, q) = 1 \implies \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$

2.3.5 Sylow 1 (Cauchy for Prime Powers)

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

Idea: Sylow p-subgroups exist for any p dividing $|G|$, and are maximal in the sense that every p-subgroup of G is contained in a Sylow p-subgroup.

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.

2.3.6 Sylow 2 (Sylows are Conjugate)

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

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

Corollary 2.11.
$n_p = 1 \iff S_p \trianglelefteq G$

2.3.7 Sylow 3 (Numerical Constraints)

1. $n_p \mathrel{\Big|} m$ (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 2.12.
p does not divide n_p.

Proposition 2.13.
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.

■

Theorem 2.14 ***(Fratini's Argument).***
If $H \trianglelefteq G$ and $P \in \mathrm{Syl}_p(G)$, then $HN_G(P) = G$ and $[G : H]$ divides $|N_G(P)|$.

2.4 Products

Theorem 2.15 ***(Recognizing Direct Products).***
We have $G \cong H \times K$ when

- $H, K \trianglelefteq G$
- $G = HK$.
- $H \bigcap K = \{e\} \subset G$

Note: can relax to $[h, k] = 1$ for all h, k.

Theorem 2.16 ***(Recognizing Generalized Direct Products).***
We have $G = \prod_{i=1}^{n} H_i$ when

- $H_i \trianglelefteq G$ for all i.
- $G = H_1 \cdots H_n$
- $H_k \bigcap H_1 \cdots \widehat{H_k} \cdots H_n = \emptyset$

Note on notation: intersect H_k with the amalgam *leaving out* H_k.

Theorem 2.17 ***(Recognizing Semidirect Products).***
We have $G = N \rtimes_\psi H$ when

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

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

Note relaxed conditions compared to direct product: $H \trianglelefteq G$ and $K \leq G$ to get a semidirect product instead

Useful Facts

- If $\sigma \in \mathrm{Aut}(H)$, then $N \rtimes_\psi H \cong N \rtimes_{\psi \circ \sigma} H$.
- $\mathrm{Aut}((\mathbb{Z}/(p)^n) \cong \mathrm{GL}(n, \mathbb{F}_p)$, which has size

$$|\mathrm{Aut}(\mathbb{Z}/(p)^n)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).$$

  - 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.

- - $\varphi(p^k) = p^{k-1}(p-1)$
- If G, H have coprime order then $\mathrm{Aut}(G \oplus H) \cong \mathrm{Aut}(G) \oplus \mathrm{Aut}(H)$.

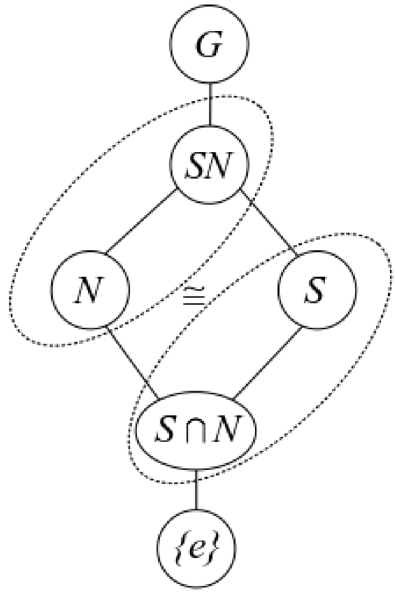


Figure 1: The 2nd "Diamond" Isomorphism Theorem

2.5 Isomorphism Theorems

Theorem 2.18 ***(1st Isomorphism Theorem).***
If $\varphi : G \longrightarrow H$ is a group morphism then

$$G/\ker\varphi \cong \text{im }\varphi.$$

Note: for this to make sense, we also have
- $\ker\varphi \trianglelefteq G$
- $\text{im }\varphi \leq G$

Corollary 2.19.
If $\varphi : G \longrightarrow H$ is surjective then $H \cong G/\ker\varphi$.

Proposition 2.20.
If $H, K \leq G$ and $H \leq N_G(K)$ (or $K \trianglelefteq G$) then $HK \leq G$ is a subgroup.

Theorem 2.21 ***(Diamond Theorem / 2nd Isomorphism Theorem).***
If $S \leq G$ and $N \trianglelefteq G$, then

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

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

Corollary 2.22.
If we relax the conditions to $S, N \leq G$ with $S \in N_G(N)$, then $S \bigcap N \trianglelefteq S$ (but is not normal in G) and the theorem still applies.

Theorem 2.23 ***(Cancellation / 3rd Isomorphism Theorem).***
Suppose $N, K \leq G$ with $N \trianglelefteq G$ and $N \subseteq K \subseteq G$.

```
1. If $K\leq G$ then $K/N \leq G/N$ is a subgroup
2. If $K\normal G$ then $K/N \normal G/N$.
3. Every subgroup of $G/N$ is of the form $K/N$ for some such $K \leq G$.
3. Every *normal* subgroup of $G/N$ is of the form $K/N$ for some such $K \normal G$.
4. If $K\normal G$, then we can cancel normal subgroups:
\[
\frac{G/N}{K/N} \cong \frac{G}{K}
.\]
```

Theorem 2.24 ***(The Correspondence Theorem / 4th Isomorphism Theorem).***
Suppose $N \trianglelefteq G$, then there exists a correspondence:

$$\left\{ H < G \,\middle|\, N \subseteq H \right\} \iff \left\{ H \,\middle|\, H < \frac{G}{N} \right\}$$
$$\left\{ \begin{array}{c} \text{Subgroups of } G \\ \text{containing } N \end{array} \right\} \iff \left\{ \begin{array}{c} \text{Subgroups of the} \\ \text{quotient } G/N \end{array} \right\}.$$

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

2.6 Special Classes of Groups

Definition 2.24.1 (2 out of 3 Property)**.**
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 2.24.2 (p-groups)**.**
If $|G| = p^k$, then G is a **p-group.**

Definition 2.24.3 (Normalizers Grow)**.**
If for every proper $H < G$, $H \trianglelefteq N_G(H)$ is again proper, then "normalizers grow" in G.

2.7 Classification of Groups

General strategy: find a normal subgroup (usually a Sylow) and use recognition of semidirect products.

- Keith Conrad: Classifying Groups of Order 12

- Order p: cyclic.
- Order $p^2 q$: ?

2.8 Finitely Generated Abelian Groups

Definition 2.24.4 (Invariant Factor Decomposition)**.**

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

Invariant factors $\longrightarrow$ Elementary Divisors:

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

Example 2.2.

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^3 \cdot 5^2 \cdot 7} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{5^2} \times \mathbb{Z}_7$$

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 2.3.
Given the invariant factor decomposition

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}$$

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

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_{3\cdot 2} \times \mathbb{Z}_{5^2\cdot 3\cdot 2}$$

Classifying Abelian Groups of a Given Order:

Let $p(x)$ be the integer partition function.

Example: $p(6) = 11$, given by $6, 5+1, 4+2, \cdots$.

Write $G = p_1^{k_1} p_2^{k_2} \cdots$; then there are $p(k_1)p(k_2)\cdots$ choices, each yielding a distinct group.

2.9 Series of Groups

Definition 2.24.5 (Normal Series)**.**
A **normal series** of a group G is a sequence $G \longrightarrow G^1 \longrightarrow G^2 \longrightarrow \cdots$ such that $G^{i+1} \trianglelefteq G_i$ for every i.

Definition 2.24.6 (Central Series)**.**
A **central series** for a group G is a terminating normal series $G \longrightarrow G^1 \longrightarrow \cdots \longrightarrow \{e\}$ such that each quotient is **central**, i.e. $[G, G^i] \leq G^{i-1}$ for all i.

Definition 2.24.7 (Composition Series)**.**
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 2.25 ***(Jordan-Holder).***
Any two composition series of a group have the same length and isomorphic composition factors (up to permutation).

Definition 2.25.1 (Simple Groups)**.**
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 G is an extension of any of its normal subgroups. I.e. for any $N \trianglelefteq G$, $G \cong E$ for some extension of the form $N \longrightarrow E \longrightarrow G/N$.

Definition 2.25.2 (Lower Central Series)**.**
Set $G^0 = G$ and $G^{i+1} = [G, G^i]$, then $G^0 \geq G^1 \geq \cdots$ is the *lower central series* of G.

Mnemonic: "lower" because the chain is descending. Iterate the adjoint map $[\cdot, G]$, if this terminates then the map is nilpotent, so call G nilpotent!

Definition 2.25.3 (Upper Central Series)**.**
Set $Z_0 = 1$, $Z_1 = Z(G)$, and $Z_{i+1} \leq G$ to be the subgroup satisfying $Z_{i+1}/Z_i = Z(G/Z_i)$. Then $Z_0 \leq Z_1 \leq \cdots$ is the *upper central series* of G.
Equivalently, since $Z_i \trianglelefteq G$, there is a quotient map $\pi : G \longrightarrow G/Z_i$, so define $Z_{i+1} \coloneqq \pi^{-1}(Z(G/Z_i))$ (?).

Mnemonic: "upper" because the chain is ascending. "Take higher centers".

Definition 2.25.4 (Derived Series)**.**
Set $G^{(0)} = G$ and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$, then $G^{(0)} \geq G^{(1)} \geq \cdots$ is the *derived series* of G.

Definition 2.25.5 (Solvable)**.**
A group G is **solvable** iff G has a terminating normal series with abelian composition factors, i.e.

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

Theorem 2.26 ***(Characterization of Solvable).***
A group G is solvable iff its derived series terminates.

Theorem 2.27 ***(S_n is Almost Always Solvable).***
If $n \geq 4$ then S_n is solvable.

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 2.27.1 (Nilpotent)**.**
A group G is **nilpotent** iff G has a terminating upper central series.

Moral: the adjoint map is nilpotent.

Theorem 2.28 ***(Nilpotents Have All Sylows Normal).***
A group G is nilpotent iff all of its Sylow p-subgroups are normal for every p dividing $|G|$.

Theorem 2.29 ***(Nilpotent Implies Maximal Normals).***
A group G is nilpotent iff every maximal subgroup is normal.

Theorem 2.30 ***(Characterization of Nilpotent Groups).***
G is nilpotent iff G has an upper central series terminating at G.

Theorem 2.31 ***(Characterization of Nilpotent Groups).***
G is nilpotent iff G has a lower central series terminating at 1.

Proposition 2.32.
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:

- Nilpotent groups satisfy the 2 out of 3 property. Specify.
- G has normal subgroups of order d for *every* d dividing $|G|$

3 Ring Theory

3.1 Definitions

3.1.1 Basics

Definition 3.0.1 (Irreducible Element)**.**
An element $r \in R$ is **irreducible** iff

$$r = ab \implies a \in R^\times \text{ or } b \in R^\times$$

Definition 3.0.2 (Prime Element)**.**
An element $p \in R$ is **prime** iff

$$a, b \in R^\times \setminus \{0\}, \quad ab \mid p \implies a \mid p \text{ or } b \mid p.$$

Example 3.1 (An irreducible element 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.

Definition 3.0.3 (Zero Divisor)**.**
An element $r \in R$ is a *zero-divisor* iff there exists an $a \in R \setminus \{0\}$ such that $ar = ra = 0$. Equivalently, the map

$$\begin{aligned} r.\,: R &\longrightarrow R \\ x &\mapsto rx \end{aligned}$$

fails to be injective.

Definition 3.0.4 (Associate Elements)**.**
$a, b \in R$ are *associates* iff there exists a $u \in R^\times$ such that $a = ub$. Equivalently, $a \mid b$ and $b \mid a$.

Definition 3.0.5 (Prime Ideal)**.**
$\mathfrak{p}$ is a **prime** ideal $\iff$

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}.$$

Definition 3.0.6 (Irreducible Ideal)**.**
An ideal $I \trianglelefteq R$ is *irreducible* if it can not be written as the intersection of two larger ideals, i.e. there are not $J_1, J_2 \supsetneq I$ such that $J_1 \bigcap J_2 = I$.

Definition 3.0.7 (Maximal Ideal)**.**
$\mathfrak{m}$ is **maximal** $\iff$ $I \ntrianglelefteq R \implies I \subseteq \mathfrak{m}$ $\iff$ R/I is a field.

Example 3.2.
Maximal ideals of $R[x]$ are of the form $I = (x - a_i)$ for some $a_i \in R$.

Definition 3.0.8 (Max Spectrum)**.**
$\text{maxSpec}\,(R) = \left\{ \mathfrak{m} \trianglelefteq R \;\middle|\; \mathfrak{m} \text{ is maximal} \right\}$ is the **max-spectrum** of R.

3.1.2 Types of Rings

Definition 3.0.9 (Integral Domain)**.**
Slogan: no nonzero zero divisors, i.e.

$$a, b \in R \setminus \{0\}, ab = 0 \implies a = 0 \text{ or } b = 0.$$

Definition 3.0.10 (Principal Ideal)**.**
$I \trianglelefteq R$ *principal* when $\exists a \in R : I = \langle a \rangle$, i.e. whenever $I \trianglelefteq R$, there is some single $a \in R$ such that $I = \langle a \rangle$.

Definition 3.0.11 (Principal Ideal Domain)**.**
A ring R is *principal* iff every ideal is principal.

Definition 3.0.12 (Unique Factorization Domain)**.**
A ring R is a *UFD* iff R is an integral domain and every $r \in R \setminus \{0\}$ admits a decomposition

$$r = u \prod_{i=1}^{n} p_i$$

where $u \in R^\times$ and the p_i irreducible, which is unique up to associates.

Definition 3.0.13 (Noetherian)**.**
A ring R is Noetherian if the ACC holds: every ascending chain of ideals $I_1 \leq I_2 \cdots$ stabilizes in the sense that there exists some N such that $I_N = I_{N+1} = \cdots$.

Definition 3.0.14 (Primary Ideal)**.**
An ideal $I \trianglelefteq R$ is *primary* iff whenever $pq \in I$, $p \in I$ and $q^n \in I$ for some n.

Definition 3.0.15 (Simple Ring)**.**
A ring R is **simple** iff every ideal $I \trianglelefteq R$ is either 0 or R.

Definition 3.0.16 (Nilradical)**.**
$\mathfrak{N}(R) := \left\{ x \in R \;\middle|\; x^n = 0 \text{ for some } n \right\}$ is the **nilradical** of R.

Definition 3.0.17 (Jacobson Radical)**.**
The **Jacobson radical** $\mathfrak{J}(R)$ is the intersection of all maximal ideals, i.e.

$$\mathfrak{J}(R) = \bigcap \mathfrak{m} \;\middle|\; \mathfrak{m} \in \operatorname{maxSpec}(R).$$

Definition 3.0.18 (Semisimple)**.**
A nonzero unital ring R is **semisimple** iff $R \cong \bigoplus_{i=1}^n M_i$ with each M_i a simple module.

Proposition 3.1 ***(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.

Proposition 3.2.
Fields $\subset$ Euclidean domains $\subset$ PIDs $\subset$ UFDs $\subset$ Integral Domains $\subset$ Rings

Example 3.3.
- 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*: $2 \mod 4$ is a zero divisor.

Proposition 3.3.
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.

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

Proposition 3.4.
If R is a PID, then every element in R has a unique prime factorization.

Theorem 3.5 ***(Krull).***
Every ring has proper maximal ideals, and any proper ideal is contained in a maximal ideal.

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

Corollary 3.6.
If M is a simple ring over R a division ring, the M is isomorphic to a matrix ring.

3.1.3 Zorn's Lemma

Theorem 3.7 ***(Zorn's Lemma).***
If P is a poset in which every chain has an upper bound, then P has a maximal element.

Some useful propositions used when *applying* Zorn's lemma:

Proposition 3.8.
Fields are simple rings.

Proposition 3.9.
If $I \trianglelefteq R$ is a proper ideal $\iff$ I contains no units.

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

■

Proposition 3.10.
If $I_1 \subseteq I_2 \subseteq \cdots$ are ideals then $\displaystyle\bigcup_j I_j$ is an ideal.

Proposition 3.11.
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 $\widehat{C} = \bigcup_i C_i$.
$\widehat{C}$ is an upper bound for C: This follows because every $C_i \subseteq \widehat{C}$.
$\widehat{C}$ is in S: Use the fact that $I \subseteq C_i < R$ for every C_i and since no C_i contains a unit, $\widehat{C}$ doesn't contain a unit, and is thus proper.

■

3.1.4 Toward Number Theory and Algebraic Geometry

Definition 3.11.1 (Reduced Ring)**.**
A ring R is *reduced* if R contains no nonzero nilpotent elements.

Definition 3.11.2 (Local Ring)**.**
A ring R is *local* iff it contains a unique maximal ideal.

Definition 3.11.3 (Prime Spectrum)**.**
$\operatorname{Spec}(R) = \left\{ \mathfrak{p} \trianglelefteq R \;\middle|\; \mathfrak{p} \text{ is prime} \right\}$ is the **spectrum** of R.

Definition 3.11.4 (Radical of an Ideal)**.**
For an ideal $I \trianglelefteq R$, the radical $\operatorname{rad}(I) \coloneqq \left\{ r \in R \;\middle|\; r^n \in I \text{ for some } n \geq 0 \right\}$, so $x^n \in I \iff x \in I$.

Definition 3.11.5 (Radical Ideal)**.**
An ideal is *radical* iff $\operatorname{rad}(I) = I$.

4 Fields

Let k denote a field.

Lemmas:

- The characteristic of any field k is either 0 or p a prime.
- All fields are simple rings (no proper nontrivial ideals).

- If L/k is algebraic, then $\min(\alpha, L)$ divides $\min(\alpha, k)$.
- Every field morphism is either zero or injective.

Theorem 4.1 ***(Finite Extensions are Algebraic).***
Every finite extension is algebraic.

Proof .
Todo

■

Theorem 4.2 ***(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 4.3.
A primitive polynomial $p \in \mathbb{Q}[x]$ is irreducible $\iff p$ is irreducible in $\mathbb{Z}[x]$.

Theorem 4.4 ***(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 over $\mathbb{Q}[x]$, and by Gauss' lemma, over $\mathbb{Z}[x]$.

Definition 4.4.1 (Primitive Extension)**.**
For R a UFD, a polynomial $p \in R[x]$ is **primitive** iff the greatest common divisors of its coefficients is a unit.

4.1 Finite Fields

Definition 4.4.2 (Prime Subfield)**.**
The **prime subfield** of a field F is the subfield generated by 1.

Theorem 4.5 ***(Characterization of Prime Subfields).***
The prime subfield of any field is isomorphic to either $\mathbb{Q}$ or $\mathbb{F}_p$ for some p.

Proposition 4.6.
If char $k = p$ then $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$.

Proof .
Todo

■

Proof

Theorem 4.7 ***(Construction of Finite Fields).***
$\mathbb{GF}(p^n) \cong \dfrac{\mathbb{F}_p}{(f)}$ where $f \in \mathbb{F}_p[x]$ is any irreducible of degree n, and $\mathbb{GF}(p^n) \cong \mathbb{F}[\alpha] \cong \operatorname{span}_{\mathbb{F}}\left\{1, \alpha, \cdots, \alpha^{n-1}\right\}$ for any root α of f.

Proposition 4.8 ***(Prime Subfields of Finite Fields).***
Every finite field F is isomorphic to a unique field of the form $\mathbb{GF}(p^n)$ and if $\operatorname{char} F = p$, it has prime subfield $\mathbb{F}_p$.

Proposition 4.9 ***(Containment of Finite Fields).***
$\mathbb{GF}(p^\ell) \leq \mathbb{GF}(p^k) \iff \ell$ divides k.

Proposition 4.10 ***(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 ρ.

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

$\blacksquare$

Proposition 4.11 ***(Splits Product of Irreducibles).***
Let $\rho_n \coloneqq x^{p^n} - x$. Then $f(x) \,\Big|\, \rho_n(x) \iff \deg f \,\Big|\, n$ and f is irreducible.

Corollary 4.12.
$x^{p^n} - x = \prod f_i(x)$ over all irreducible monic $f_i \in \mathbb{F}_p[x]$ of degree d dividing n.

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

- $\alpha \in \mathbb{GF}(p^n) \iff \alpha^{p^n} - \alpha = 0$, so every element is a root of φ_n and $\deg \min(\alpha, \mathbb{F}_p) \,\Big|\, n$ 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 $\deg f \,\Big|\, n$. $\varphi_n'(x) = p^n x^{p^{n-1}} \neq 0$, so φ_n has distinct roots and thus no repeated factors. So φ_n is the product of all such irreducible f.

$\blacksquare$

Proposition 4.13.
No finite field is algebraically closed.

Proof .
Todo

$\blacksquare$

Proof

4.2 Galois Theory

Definition 4.13.1 (Algebraic Field Extension).
A field extension L/k is **algebraic** iff every $\alpha \in L$ is the root of some polynomial $f \in k[x]$.

Definition 4.13.2 (Normal Field Extension).
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 4.13.3 (Separable Field Extension).
Let L/k be a field extension, $\alpha \in L$ be arbitrary, and $f(x) \coloneqq \min(\alpha, k)$. TFAE:

- L/k is **separable**
- f has no repeated factors/roots
- $\gcd(f, f') = 1$, i.e. f is coprime to its derivative
- $f' \not\equiv 0$

Proposition 4.14.
If char $k = 0$ or k is finite, then every *algebraic* extension L/k is separable.

Definition 4.14.1 (Field Automorphisms).
$\mathrm{Aut}(L/k) = \left\{ \sigma : L \longrightarrow L \;\middle|\; \sigma|_k = \mathrm{id}_k \right\}$.

Proposition 4.15.
If L/k is algebraic, then $\mathrm{Aut}(L/k)$ permutes the roots of irreducible polynomials.

Proposition 4.16.
$|\mathrm{Aut}(L/k)| \leq [L : k]$ with equality precisely when L/k is normal.

Definition 4.16.1 (Galois Group).
If L/k is Galois, we define $\mathrm{Gal}(L/k) \coloneqq \mathrm{Aut}(L/k)$.

4.2.1 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):* $\min(\alpha, F) \Big| \min(\alpha, k)$, 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 $E_1 \bigcap E_2/k$ normal.

$$
\begin{tikzcd}
L \arrow[d, dotted, bend right] \arrow[dd, bend left] \\
F \\
k
\end{tikzcd}
$$

- 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

$$
\begin{tikzcd}
L \arrow[d, bend right] \arrow[dd, dashed, bend left] \\
F \arrow[d, bend right] \\
k
\end{tikzcd}
$$

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

$$
\begin{tikzcd}
L \arrow[d, dotted, bend right] \arrow[dd, bend left] \\
F \arrow[d, bend right] \\
k
\end{tikzcd}
$$

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 4.16.2 (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
- $|\mathrm{Aut}(L/k)| = [L : k]$
- The fixed field of $\mathrm{Aut}(L/k)$ is exactly k.

Theorem 4.17 ***(Fundamental Theorem of Galois Theory).***

Let L/k be a Galois extension, then there is a correspondence:

$$\left\{\text{Subgroups } H \le \mathrm{Gal}(L/k)\right\} \iff \left\{\substack{\text{Fields } F \text{ such} \\ \text{that } L/F/k}\right\}$$
$$H \to \left\{E^H := \text{ The fixed field of } H\right\}$$
$$\left\{\mathrm{Gal}(L/F) := \left\{\sigma \in \mathrm{Gal}(L/k) \;\middle|\; \sigma(F) = F\right\}\right\} \leftarrow F$$

- 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 $Gal(K/F) = H$
- F/k is Galois $\iff$ H is normal, and $\mathrm{Gal}(F/k) = \mathrm{Gal}(L/k)/H$.
- The compositum F_1F_2 corresponds to $H_1 \bigcap H_2$.
- The subfield $F_1 \bigcap F_2$ corresponds to H_1H_2.

4.2.2 Examples

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

I.e., the following map is an isomorphism:

$$\begin{aligned} \mathbb{Z}/(n)^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q}) \\ r \mod n &\mapsto (\varphi_r : \zeta_n \mapsto \zeta_n^r) \end{aligned}$$

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

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

Proposition 4.18.
Every quadratic extension is Galois.

Proposition 4.19.
If K is the splitting field of an irreducible polynomial of degree n, then $\mathrm{Gal}(K/\mathbb{Q}) \le S_n$ is a transitive subgroup.

Corollary 4.20.
n divides the order $|\mathrm{Gal}(K/\mathbb{Q})|$.

Theorem 4.21 ***(Characterization of Perfect Fields).***
TFAE:

- k is a **perfect** field.
- Every irreducible polynomial $p \in k[x]$ is separable

- Every finite extension F/k is separable.
- If char $k > 0$, the Frobenius is an automorphism of k.

Theorem 4.22 ***(Splitting + Perfect implies Galois).***

- If 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.

Proposition 4.23 ***(Composite Extensions).***
If F/k is finite and Galois and L/k is arbitrary, then FL/L is Galois and

$$\mathrm{Gal}(FL/L) = \mathrm{Gal}(F/F \bigcap L) \subset \mathrm{Gal}(F/k).$$

4.3 Cyclotomic Polynomials

Definition 4.23.1 (Cyclotomic Polynomials)**.**
Let $\zeta_n = e^{2\pi i/n}$, then the n**th cyclotomic polynomial** is given by

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

which is a product over primitive roots of unity. It is the unique irreducible polynomial which is a divisor of $x^n - 1$ but *not* a divisor of $x^k - 1$ for any $k < n$.

Proposition 4.24.
$\deg \Phi_n(x) = \varphi(n)$ for φ the totient function.

Proof .
$\deg \Phi_n(x)$ is the number of nth primitive roots, which is the number of numbers less than and coprime to n.

■

Computing Φ_n:

1.

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

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.

Proposition 4.25.

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$
$$\Phi_{2p}(x) = x^{p-1} - x^{p-2} + \cdots - x + 1$$

Proposition 4.26.

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

Definition 4.26.1 (Simple Extension)**.**
An extension F/k is **simple** if $F = k[\alpha]$ for a single element α.

Theorem 4.27 ***(Primitive Element).***
Every finite separable extension is simple.

Corollary 4.28.
$\mathbb{GF}(p^n)$ is a simple extension over $\mathbb{F}_p$.

5 Modules

5.1 General Modules

Definition (Simple Module) A module is **simple** iff it has no nontrivial proper submodules.

Definition (Free Module) 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 (Projective Module) 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 (Exact Sequences) A sequence of module morphisms $0 \xrightarrow{d_1} A \xrightarrow{d_2} B \xrightarrow{d_3} C \longrightarrow 0$ is *exact* iff $\operatorname{im} d_i = \ker d_{i+1}$.

Proposition (Splitting Exact Sequences) If $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ 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 $B \cong A \oplus C$.

5.2 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.

Proposition (Principal Ideals are Free) $I \trianglelefteq R$ 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.

$\impliedby$:

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.

6 Linear Algebra

Definition (Invariant Factor) ?
Definition (Elementary Divisor) ?

6.1 Minimal / Characteristic Polynomials

Fix some notation:

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

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

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

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

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 $\chi_A(A) = 0$.

Proof By Cayley-Hamilton, $\min_A$ divides χ_A. Every λ_i is a root of μ_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 (Similar Matrices) Two matrices A, B are **similar** (i.e. $A = PBP^{-1}$) $\iff$ A, B have the same Jordan Canonical Form (JCF).

Definition (Equivalent Matrices) 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)

6.2 Finding Minimal Polynomials

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 $T\mathbf{v}, T^2\mathbf{v}, \cdots T^k\mathbf{v}$ until a linear dependence is introduced. Write this as $p(T) = 0$; then $\min_A(x) \mid p(x)$.

Definition (Companion Matrix) Given a monic $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} + x^n$, the **companion matrix** of p is given by

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

6.3 Canonical Forms

6.3.1 Rational Canonical Form

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

Theorem (Structure Theorem) For R a PID and M a finitely-generated R-module, there exists an invariant factor decomposition

$$M \cong R^r \bigoplus_{i=1}^{\ell} R/(a_i) \quad a_1 \mid a_2 \mid \cdots \mid a_\ell$$

where each a_i is an invariant factor.

Proposition Each a_i corresponds

Proposition (RCF Relates to Invariant Factors) $RCF(A)$ is a block matrix where each block is the companion matrix of an invariant factor of A.

Proof The derivation:

- Let $k[x] \curvearrowright V$ using T, makes V into a $k[x]$-module.
- k a field implies $k[x]$ a PID, so apply structure theorem to obtain 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 span $\{\overline{x}\} = F[x]/(a_i)$.
- Write $a_i(x) = \sum b_i x^i$, note that $V \longrightarrow F[x]$ 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.

6.3.2 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 (JCF from Minimal and Characteristic Polynomials) Writing Spec $(A) = \{(\lambda_i, b_i)\}$,

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

- The roots both polynomials are precisely the eigenvalues of A
- The spectrum of A corresponds precisely to the **characteristic** polynomial
- $a_i \leq b_i$
- a_i is 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 and the number of times λ_i appears on the diagonal of $JCF(A)$.
- $\dim E_{\lambda_i}$ is the **number of Jordan blocks** associated to λ_i

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

6.5 Diagonalizability

Notation: A^* denotes the conjugate tranpose of A.

Lemma Let V be a vector space over k an algebraically closed and $A \in \operatorname{End}(V)$. 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) Statements:

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, $\mathbf{v} \in V$.

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

Proposition (Simultaneous Diagonalizability) A set of operators $\{A_i\}$ 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.

6.6 Matrix Counterexamples

1. A matrix that:

- Is not diagonalizable over $\mathbb{R}$ but diagonalizable over $\mathbb{C}$
- Has *no* eigenvalues over $\mathbb{R}$ but has *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:

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

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

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

Proof Let $a \in R$ and define $\varphi(x) = ax$. 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.

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

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 $ab \in \mathfrak{m} \implies a \in \mathfrak{m}$.

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.

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

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

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 $S = \left\{ I \trianglelefteq R \;\middle|\; a^n \not\in I \text{ for any } n \right\}$. 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

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

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

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

7 Extra Problems

7.1 Group Theory

7.1.1 Basic Structure

Just Structure

- Show that the intersection of two subgroups is again a subgroup.
- Show that the intersection of two subgroups with coprime orders is trivial.
- Show that subgroups with the *same* prime order are either equal or intersect trivially.
- Give a counterexample where $H, K \leq G$ but HK is not a subgroup of G.
- Show that $G = H \times K$ iff the conditions for recognizing direct products hold.
- Show that if $H, K \trianglelefteq G$ and $H \bigcap K = \emptyset$, then $hk = kh$ for all $h \in H, k \in K$.
- Show that if $H, K \trianglelefteq G$ are normal subgroups that intersect trivially, then $[H, K] = 1$ (so $hk = kh$ for all k and h).
- Show that the order of any element in a group divides the order of the group.
- Show that the size of a conjugacy class divides the order of a group.
- Show that $|G|/|H| = [G : H]$.

Centers

- Show that if $G/Z(G)$ is cyclic then G is abelian.
- Show that G/N is abelian iff $[G, G] \leq N$.

- Show that every normal subgroup of G is contained in $Z(G)$.

Cyclic Groups

- Show that any cyclic group is abelian.
- Show that every subgroup of a cyclic group is cyclic.
- Show that

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

- Compute $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$ for n composite.
- Compute $\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$.

  Hint: Orbit-stabilizer

7.1.2 Centralizing and Normalizing

- Show that $C_G(H) \subseteq N_G(H) \leq G$.
- Show that $Z(G) \subseteq C_G(H) \subseteq N_G(H)$.
- Given $H \subseteq G$, let $S(H) = \bigcup_{g \in G} gHg^{-1}$, so $|S(H)|$ is the number of conjugates to H. Show that $|S(H)| = [G : N_G(H)]$.
  - That is, the number of subgroups conjugate to H equals the index of the normalizer of H.
- Show that $Z(G) = \bigcap_{a \in G} C_G(a)$.
- Show that the centralizer $G_G(H)$ of a subgroup is again a subgroup.
- Show that $C_G(H) \trianglelefteq N_G(H)$ is a normal subgroup.
- Show that $C_G(G) = Z(G)$.
- Show that for $H \leq G$, $C_H(x) = H \bigcap C_G(x)$.
- Let $H, K \leq G$ a finite group, and without using the normalizers of H or K, show that $|HK| = |H||K| / \left| H \bigcap K \right|$.
- Show that if $H \leq N_G(K)$ then $HK \leq H$, and give a counterexample showing that this condition is necessary.
- Show that HK is a subgroup of G iff $HK = KH$.
- Prove that the kernel of a homomorphism is a normal subgroup.

7.1.3 Primes in Group Theory

- Show that any group of prime order is cyclic and simple.
- Analyze groups of order pq with $q < p$.

  Hint: consider the cases when p does or does not divide $q - 1$.

  - Show that if q does not divide $p - 1$, then G is cyclic.
  - Show that G is never simple.
- Analyze groups of order p^2q.

  Hint: Consider the cases when q does or does not divide $p^2 - 1$.
- Show that no group of order p^2q^2 is simple for $p < q$ primes.
- Show that a group of order p^2q^2 has a normal Sylow subgroup.
- Show that a group of order p^2q^2 where q does not divide $p^2 - 1$ and p does not divide $q^2 - 1$ is abelian.
- Show that every group of order pqr with $p < q < r$ primes contains a normal Sylow subgroup.
  - Show that G is never simple.
- Show that any normal p- subgroup is contained in every Sylow p-subgroup of G.

7.1.4 p-Groups

- Show that every p-group has a nontrivial center.
- Show that every p-group is nilpotent.
- Show that every p-group is solvable.
- Show that every maximal subgroup of a p-group has index p.
- Show that every maximal subgroup of a p-group is normal.
- Show that every group of order p is cyclic.
- Show that every group of order p^2 is abelian and classify them.
- Show that every normal subgroup of a p-group is contained in the center.

  Hint: Consider $G/Z(G)$.
- Let $O_P(G)$ be the intersection of all Sylow p-subgroups of G. Show that $O_p(G) \trianglelefteq G$, is maximal among all normal p-subgroups of G
- Let $P \in \mathrm{Syl}_p(H)$ where $H \trianglelefteq G$ and show that $P \bigcap H \in \mathrm{Syl}_p(H)$.
- Show that Sylow p_i-subgroups S_{p_1}, S_{p_2} for distinct primes $p_1 \neq p_2$ intersect trivially.

7.1.5 Symmetric Groups

Specific Groups

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

General Structure

- Show that an m-cycle is an odd permutation iff m is an even number.
- Show that a permutation is odd iff it has an odd number of even cycles.
- Show that the center of S_n for $n \geq 4$ is nontrivial.
- Show that disjoint cycles commute.
- Show directly that any k-cycle is a product of transpositions, and determine how many transpositions are needed.

Generating Sets

- Show that S_n is generated by any of the following types of cycles:

Group	Generating Set	Size
S_n, $n \geq 2$	(ij)'s	$\frac{n(n-1)}{2}$
	$(12), (13), \ldots, (1n)$	$n-1$
	$(12), (23), \ldots, (n-1\ n)$	$n-1$
	$(12), (12\ldots n)$ if $n \geq 3$	2
	$(12), (23\ldots n)$ if $n \geq 3$	2
	$(ab), (12\ldots n)$ if $(b-a, n) = 1$	2
A_n, $n \geq 3$	3-cycles	$\frac{n(n-1)(n-2)}{3}$
	$(1ij)$'s	$(n-1)(n-2)$
	$(12i)$'s	$n-2$
	$(i\ i+1\ i+2)$'s	$n-2$
	$(123), (12\ldots n)$ if $n \geq 4$ odd	2
	$(123), (23\ldots n)$ if $n \geq 4$ even	2

  - Show that S_n is generated by transpositions.
  - Show that S_n is generated by *adjacent* transpositions.
  - Show that S_n is generated by $\{(12), (12\cdots n)\}$ for $n \geq 2$

- Show that S_n is generated by $\{(12), (23 \cdots n)\}$ for $n \geq 3$
- Show that S_n is generated by $\{(ab), (12 \cdots n)\}$ where $1 \leq a < b \leq n$ iff $\gcd(b - a, n) = 1$.
- Show that S_p is generated by any arbitrary transposition and any arbitrary p-cycle.

7.1.6 Alternating Groups

- Show that A_n is generated 3-cycles.
- Prove that A_n is normal in S_n.
- Argue that A_n is simple for $n \geq 5$.
- Show that $\mathrm{Out}(A_4)$ is nontrivial.

7.1.7 Dihedral Groups

- Show that if $N \trianglelefteq D_n$ is a normal subgroup of a dihedral group, then D_n/N is again a dihedral group.

7.1.8 Other Groups

- Show that $\mathbb{Q}$ is not finitely generated as a group.
- Show that the Quaternion group has only one element of order 2, namely -1.

7.1.9 Classification

- Show that no group of order 36 is simple.
- Show that no group of order 90 is simple.
- Show that all groups of order 45 are abelian.
- Classify all groups of order 10.
- Classify the five groups of order 12.
- Classify the four groups of order 28.
- Show that if $|G| = 12$ and has a normal subgroup of order 4, then $G \cong A_4$.

7.1.10 Group Actions

- Show that the stabilizer of an element G_x is a subgroup of G.
- Show that if x, y are in the same orbit, then their stabilizers are conjugate.
- Show that the stabilizer of an element need not be a normal subgroup?
- Show that if $G \curvearrowright X$ is a group action, then the stabilizer G_x of a point is a subgroup.

7.1.11 Series of Groups

- Show that A_n is simple for $n \geq 5$
- Give a necessary and sufficient condition for a cyclic group to be solvable.
- Prove that every simple abelian group is cyclic.
- Show that S_n is generated by disjoint cycles.
- Show that S_n is generated by transpositions.

- Show if G is finite, then G is solvable $\iff$ all of its composition factors are of prime order.
- Show that if N and G/N are solvable, then G is solvable.
- Show that if G is finite and solvable then every composition factor has prime order.
- Show that G is solvable iff its derived series terminates.
- Show that S_3 is not nilpotent.
- Show that G nilpotent $\implies$ G solvable
- Show that nilpotent groups have nontrivial centers.
- Show that Abelian $\implies$ nilpotent
- Show that p-groups $\implies$ nilpotent

7.1.12 Misc

- Prove Burnside's theorem.
- Show that $\mathrm{Inn}(G) \trianglelefteq Aut(G)$
- Show that $\mathrm{Inn}(G) \cong G/Z(G)$
- Show that the kernel of the map $G \longrightarrow \mathrm{Aut}(G)$ given by $g \mapsto (h \mapsto ghg^{-1})$ is $Z(G)$.
- Show that $N_G(H)/C_G(H) \cong A \leq Aut(H)$
- Give an example showing that normality is not transitive: i.e. $H \trianglelefteq K \trianglelefteq G$ with H *not* normal in G.

7.1.13 Nonstandard Topics

- Show that H char $G \Rightarrow H \trianglelefteq G$

  > Thus "characteristic" is a strictly stronger condition than normality

- Show that H char K char $G \Rightarrow H$ char G

  > So "characteristic" is a transitive relation for subgroups.

- Show that if $H \leq G$, $K \trianglelefteq G$ is a normal subgroup, and H char K then H is normal in G.

  > So normality is not transitive, but strengthening one to "characteristic" gives a weak form of transitivity.

7.2 Ring Theory

Basic Structure

- Show that if an ideal $I \trianglelefteq R$ contains a unit then $I = R$.
- Show that $R^\times$ need not be closed under addition.

Ideals

- Show that every proper ideal is contained in a maximal ideal

- Show that if $x \in R$ a PID, then x is irreducible $\iff \langle x \rangle \trianglelefteq R$ is maximal.
- Show that intersections, products, and sums of ideals are ideals.
- Show that the union of two ideals need not be an ideal.
- Show that every ring has a proper maximal ideal.
- Show that $I \trianglelefteq R$ is maximal iff R/I is a field.
- Show that $I \trianglelefteq R$ is prime iff R/I is an integral domain.
- Show that $\displaystyle\bigcup_{\mathfrak{m} \in \text{maxSpec }(R)} = R \setminus R^\times$.
- Show that maxSpec $(R) \subsetneq$ Spec (R) but the containment is strict.
- Show that if x is not a unit, then x is contained in some maximal ideal.
- Show that if R is a finite ring then every $a \in R$ is either a unit or a zero divisor.
- Show that $R/\mathfrak{N}(R)$ has no nonzero nilpotent elements.
- Show that the nilradical is contained in the Jacobson radical.
- Show that every prime ideal is radical.
- Show that the nilradical is given by $\mathfrak{N}(R) = \text{rad }(0)$.
- Show that $\text{rad}(IJ) = \text{rad}(I) \bigcap \text{rad}(J)$
- Show that if Spec $(R) \subseteq$ maxSpec (R) then R is a UFD.
- Show that if R is Noetherian then every ideal is finitely generated.

Characterizing Certain Ideals

- Show that the nilradical is the intersection of all prime ideals.
- Show that for an ideal $I \trianglelefteq R$, its radical is the intersection of all prime ideals containing I.
- Show that rad (I) is the intersection of all prime ideals containing I.

Misc

- Show that localizing a ring at a prime ideal produces a local ring.
- Show that R is a local ring iff for every $x \in R$, either x or $1 - x$ is a unit.
- Show that if R is a local ring then $R \setminus R^\times$ is a proper ideal that is contained in $\mathfrak{J}(R)$.
- Show that if $R \neq 0$ is a ring in which every non-unit is nilpotent then R is local.
- Show that every prime ideal is primary.
- Show that every prime ideal is irreducible.
- Show that

7.3 Field Theory

General Algebra

- Show that any finite integral domain is a field.
- Show that every field is simple.
- Show that any field morphism is either 0 or injective.
- Show that if L/F and α is algebraic over both F and L, then the minimal polynomial of α over L divides the minimal polynomial over F.
- Prove that if R is an integral domain, then $R[t]$ is again an integral domain.
- Show that $ff(R[t]) = ff(R)(t)$.

Extensions?

- What is $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}]$?
- What is $[\mathbb{Q}(2^{\frac{3}{2}}) : \mathbb{Q}]$?

- Show that if $p \in \mathbb{Q}[x]$ and $r \in \mathbb{Q}$ is a rational root, then in fact $r \in \mathbb{Z}$.
- If $\{\alpha_i\}_{i=1}^n \subset F$ are algebraic over K, show that $K[\alpha_1, \cdots, \alpha_n] = K(\alpha_1, \cdots, \alpha_n)$.
- Show that α/F is algebraic $\iff$ $F(\alpha)/F$ is a finite extension.
- Show that every finite field extension is algebraic.
- Show that if α, β are algebraic over F, then $\alpha \pm \beta, \alpha\beta^{\pm 1}$ are all algebraic over F.
- Show that if $L/K/F$ with K/F algebraic and L/K algebraic then L is algebraic.

Special Polynomials

- Show that a field with p^n elements has exactly one subfield of size p^d for every d dividing n.
- Show that $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n.
- Show that $x^{p^d} - x \mid x^{p^n} - x \iff d \mid n$
- Prove that $x^{p^n} - x$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ with degree dividing n.
- Prove that an irreducible $\pi(x) \in \mathbb{F}_p[x]$ divides $x^{p^n} - x \iff \deg \pi(x)$ divides n.

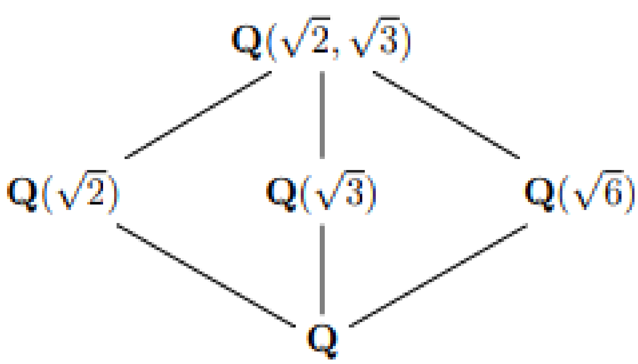
7.4 Galois Theory

7.4.1 Theory

- Show that if K/F is the splitting field of a separable polynomial then it is Galois.
- Show that any quadratic extension of a field F with char $(F) \neq 2$ is Galois.
- Show that if $K/E/F$ with K/F Galois then K/E is always Galois with $g(K/E) \leq g(K/F)$.
  - Show additionally E/F is Galois $\iff$ $g(K/E) \trianglelefteq g(K/F)$.
  - Show that in this case, $g(E/F) = g(K/F)/g(K/E)$.
- Show that if $E/k, F/k$ are Galois with $E \bigcap F = k$, then EF/k is Galois and $G(EF/k) \cong G(E/k) \times G(F/k)$.

7.4.2 Computations

- Show that the Galois group of $x^n - 2$ is D_n, the dihedral group on n vertices.
- Compute all intermediate field extensions of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, show it is equal to $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, and find a corresponding minimal polynomial.



- Compute all intermediate field extensions of $\mathbb{Q}(2^{\frac{1}{4}}, \zeta_8)$.
- Show that $\mathbb{Q}(2^{\frac{1}{3}})$ and $\mathbb{Q}(\zeta_3 2^{\frac{1}{3}})$

- Show that if L/K is separable, then L is normal $\iff$ there exists a polynomial $p(x) = \prod_{i=1}^{n} x - \alpha_i \in K[x]$ such that $L = K(\alpha_1, \cdots, \alpha_n)$ (so L is the splitting field of p).
- Is $\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}$ normal?
- Show that $\mathbb{GF}(p^n)$ is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.
- Show that $\mathbb{GF}(p^d) \leq \mathbb{GF}(p^n) \iff d \mid n$
- Compute the Galois group of $x^n - 1 \in \mathbb{Q}[x]$ as a function of n.
- Identify all of the elements of the Galois group of $x^p - 2$ for p an odd prime (note: this has a complicated presentation).
- Show that $\mathrm{Gal}(x^{15} + 2)/\mathbb{Q} \cong S_2 \rtimes \mathbb{Z}/15\mathbb{Z}$ for S_2 a Sylow 2-subgroup.
- Show that $\mathrm{Gal}(x^3 + 4x + 2)/\mathbb{Q} \cong S_3$, a symmetric group.

7.5 Modules and Linear Algebra

- Prove the Cayley-Hamilton theorem.
- Prove that the minimal polynomial divides the characteristic polynomial.
- Prove that the cokernel of $A \in \mathrm{Mat}(n \times n, \mathbb{Z})$ is finite $\iff \det A \neq 0$, and show that in this case $|\mathrm{coker}(A)| = |\det(A)|$.
- Show that a nilpotent operator is diagonalizable.
- Show that if A, B are diagonalizable and $[A, B] = 0$ then A, B are simultaneously diagonalizable.
- Does diagonalizable imply invertible? The converse?
- Does diagonalizable imply distinct eigenvalues?
- Show that if a matrix is diagonalizable, its minimal polynomial is squarefree.
- Show that a matrix representing a linear map $T : V \longrightarrow V$ is diagonalizable iff V is a direct sum of eigenspaces $V = \bigoplus_i \ker(T - \lambda_i I)$.
- Show that if $\{\mathbf{v}_i\}$ is a basis for V where $\dim(V) = n$ and $T(\mathbf{v}_i) = \mathbf{v}_{i+1 \mod n}$ then T is diagonalizable with minimal polynomial $x^n - 1$.
- Show that if the minimal polynomial of a linear map T is irreducible, then every T-invariant subspace has a T-invariant complement.

7.6 Commutative Algebra

- Show that a finitely generated module over a Noetherian local ring is flat iff it is free using Nakayama and Tor.