Algebra Qualifying Exam Review

D. Zack Garza

Table of Contents

Contents

1 Topics and Remarks 2

Remark 1.0.1: 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 General References

- David Dummit and Richard Foote, Abstract Algebra, Wiley, 2003. [1]
- Kenneth Hoffman and Ray Kunze, Linear Algebra, Prentice-Hall, 1971. [2]
- Thomas W. Hungerford, Algebra, Springer, 1974. [3]
- Roy Smith, Algebra Course Notes (843-1 through 845-3). [4]
  - Note: scroll down the page to find links to his course notes.

1.2 Group Theory

References: [1], [3], [4] "The first 6 chapters (220 pages) of D definitions and proofs of these theorems on groups are given in 843 part 1."

1.2.1 Key Topics

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

1.2.2 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]

1.3.1 Key Topics

- 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]

1.4.1 Key Topics

- 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)

1.4.2 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 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]

1.5.1 Key Topics

- 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

1.6.1 Key Topics

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

2.1 Big List of Notation

Notation	Definition
$C_G(x)$	Centralizer of an element $\coloneqq \left\{ g \in \Gamma \;\middle|\; [g,x] = 1 \right\} \subseteq \Gamma$
$C_G(H)$	Centralizer of an subgroup $\coloneqq \left\{ g \in \Gamma \;\middle|\; [g,x] = 1 \ \forall h \in H \right\} = \bigcap_{h \in H} C_H(h) \subseteq G$
$C(H)$	Conjugacy Class $\coloneqq \left\{ ghg^{-1} \;\middle|\; g \in G \right\} \leq G \subseteq G$
$Z(G)$	Center $\coloneqq \left\{ x \in G \;\middle|\; \forall g \in G,\, gxg^{-1} = x \right\} \subseteq G$
$N_G(H)$	Normalizer $\coloneqq \left\{ g \in G \;\middle|\; gHg^{-1} = H \right\} \subseteq G$

Notation	Definition
$\mathrm{Inn}(G)$	Inner Automorphisms $\coloneqq \left\{\varphi_g(x) \coloneqq gxg^{-1}\right\} \subseteq \mathrm{Aut}(G)$
$\mathrm{Out}(G)$	Outer Automorphisms $\mathrm{Aut}(G)/\mathrm{Inn}(G) \hookleftarrow \mathrm{Aut}(G)$
$[gh]$	Commutator of Elements $\coloneqq ghg^{-1} \in G$
$[GH]$	Commutator of Subgroups $\coloneqq \left\langle \left\{ [gh] \;\middle|\; g \in G,\, h \in H \right\} \right\rangle \leq G$
$\mathcal{O}_x$, Gx	Orbit of an Element $\coloneqq \left\{ gx \;\middle|\; x \in X \right\}$
$\mathrm{Stab}_G(x)$, G_x	Stabilizer of an Element $\coloneqq \left\{ g \in G \;\middle|\; gx = x \right\} \subseteq G$
X/G	Set of Orbits $\coloneqq \left\{ G_x \;\middle|\; x \in X \right\} \subseteq 2^X$
X^g	Fixed Points $\left\{ x \in X \;\middle|\; \forall g \in G,\, gx = x \right\} \subseteq X$
2^X	The powerset of X $\coloneqq \{U \subseteq X\}$

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

2.2 Definitions

Definition 2.2.1 (Subgroup Generated by a Subset)
If $H \subset G$, then $\langle H \rangle$ is the smallest subgroup containing H:

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

Definition 2.2.2 (Centralizer)

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

Definition 2.2.3 (Normalizer)

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

Definition 2.2.4 (The Dihedral Group)
A **dihedral group** of order $2n$ is given by

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

Definition 2.2.5 (Alternating Group)
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 $\operatorname{sign}(\sigma) = (-1)^m$ and m is the number of cycles of even length.

Definition 2.2.6 (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 2.2.7 (Transitive Subgroup)
A subgroup of S_n is **transitive** iff its action on $\{1, 2, \cdots, n\}$ is transitive.

2.3 Subgroups and Quotients

Fact 2.3.1
Coprime order subgroups are disjoint, or more generally $\mathbb{Z}_p, \mathbb{Z}_q \subset G \implies \mathbb{Z}_p \cap \mathbb{Z}_q = \mathbb{Z}_{(p,q)}$.

Theorem 2.3.2 ***(The Fundamental Theorem of Cosets).***

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

Theorem 2.3.3 ***(Counting Quotients).***
If $H \trianglelefteq G$, then

$$[G : H] = |G/H| = \frac{|G|}{|H|}.$$

Theorem 2.3.4 ***(Counting by Towers).***

$$[G : K] = [G : H]\,[H : K].$$

2.4 Special Classes of Groups

2.4.1 Cyclic Groups

Theorem 2.4.1 ***(Subgroups of Cyclic Groups).***
If G is cyclic of order n, G has a unique subgroup of order d for each d dividing n.

2.4.2 The Symmetric Group

Definition 2.4.2 (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 $k-1$.

Corollary 2.4.3 ***(Alternating Group).***
Every $\sigma \in A_n$ has an even number of *odd* cycles (i.e. an even number of *even-length* cycles).

Example 2.4.4:

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

Fact 2.4.5 (Some 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*.

2.5 Counting Theorems

Theorem 2.5.1 ***(Lagrange's Theorem).***

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

Corollary 2.5.2.
The order of every element divides the size of G, i.e.

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

⚠ **Warning 2.5.3**
There does **not** necessarily exist $H \leq G$ with $|H| = n$ for every $n \mid |G|$. Counterexample: $|A_4| = 12$ but has no subgroup of order 6.

Theorem 2.5.4 ***(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 strengthene

2.5.1 Group Actions

Definition 2.5.5 (Group Action)
An action of G on X is a group morphism

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

or equivalently

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

satisfying

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

Fact 2.5.6
$\ker \psi = \cap_{x \in X} G_x$ is the intersection of all stabilizers.

Definition 2.5.7 (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.

Remark 2.5.8 ***(Reminder of notation):*** For a group G acting on a set X,

Notation	Definition
$G \cdot x = \left\{ g \cdot x \;\middle|\; g \in G \right\} \subseteq X$	Orbit
$G_x = \left\{ g \in G \;\middle|\; gx = x \right\} \leq G$	Stabilizer
$X/G \subseteq 2^X$	Set of Orbits
$X^g = \left\{ x \in X \;\middle|\; g \cdot x = x \right\} \subseteq X$	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 2.5.9 ***(Orbit-Stabilizer).***

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

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

2.5.2 Examples of Orbit-Stabilizer and the Class Equation

Example 2.5.10 ***(Trivial):*** Let G act on itself by left translation, where $g \mapsto (h \mapsto gh)$.

- The orbit $\mathcal{O}_x = Gx = G$ is the entire group
- The stabilizer $G_x = \{e\}$ is only the identity.
- The set of fixed points $X^g = \{e\}$ is only the identity.

Example 2.5.11 ***(Conjugation yields centers/centralizers):*** Let G act on *itself* by conjugation.

- The orbit $\mathcal{O}_x = Gx = C(x)$ is the **conjugacy class** of x.
  - Note that this means this action is not necessarily transitive.
- $G_x = Z(x) \coloneqq C_G(x) = \left\{ g \in G \;\middle|\; [g, x] = e \right\}$, the **centralizer** of x.

- The set of fixed points $X^g = Z(G)$ is the **center**.

Corollary 2.5.12.
The number of conjugates of an element (i.e. the size of its conjugacy class) is the index of its centralizer, $[G : C_G(x)]$, i.e.

$$|C(x)| = [G : C_G(x)].$$

Corollary 2.5.13 ***(The Class Equation).***

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

Remark 2.5.14: 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.

Example 2.5.15 ***(?):*** Let G act on $X \coloneqq \left\{H \;\middle|\; H \leq G\right\}$ (its set of *subgroups*) by conjugation. Let $x = H$ be a subgroup, then

- The orbit $Gx = \left\{gHg^{-1}\right\}$ is the **set of conjugate subgroups** of H
- The stabilizer $G_x = N_G(H)$ is the **normalizer** of in G of H
- The fixed points X^g is the set of **normal subgroups** of G

Corollary 2.5.16.
Given $H \leq G$, the number of conjugate subgroups is $[G : N_G(H)]$, i.e.

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

Example 2.5.17 ***(?):*** For a fixed proper subgroup $H < G$, let G act on its cosets $X \coloneqq G/H \coloneqq \left\{gH \;\middle|\; g \in G\right\}$ by left translation. Let $x \coloneqq gH$, then

- The orbit $Gx = G/H$, the entire set of cosets.
  - Note that this is a *transitive* action.
- The stabilizer $G_x = gHg^{-1}$, a **conjugate subgroup** of H
- The fixed points are $X^G = \varnothing$

Proposition 2.5.18 ***(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 $\ker \varphi = 1$.

■

Corollary 2.5.19 ***(Burnside's Formula).***
For G a finite group acting on X,

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

Mnemonic: the number of orbits is equal to the average number o

Proof (?).

$$\begin{aligned}
\sum_{g \in G} |X^g| &= \left\{ (g, x) \in G \times X \;\middle|\; gx = x \right\} \\
&= \sum_{x \in X} |G_x| \\
&= \sum_{x \in X} \frac{|G|}{|Gx|} && \text{by Orbit-Stabilizer} \\
&= |G| \sum_{x \in X} \frac{1}{|Gx|} \\
&= |G| \sum_{A \in X/G} \sum_{x \in A} \frac{1}{|A|} && \text{since } X = \coprod_{A \in X/G} A \\
&= |G| \sum_{A \in X/G} 1 \\
&= |G||X/G|.
\end{aligned}$$

■

2.6 Isomorphism Theorems

Theorem 2.6.1 ***(1st Isomorphism Theorem).***
If $\varphi : G \to H$ is a group morphism then

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

Note: for this to make sense, we also have

- $\ker \varphi \trianglelefteq G$
- $\operatorname{im} \varphi \leq G$

Corollary 2.6.2.
If $\varphi : G \to H$ is surjective then $H \cong G/\ker \varphi$.

Theorem 2.6.3 ***(Diamond Theorem / 2nd Isomorphism Theorem).***
If $S \leq G$ and $N \trianglelefteq G$, then

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

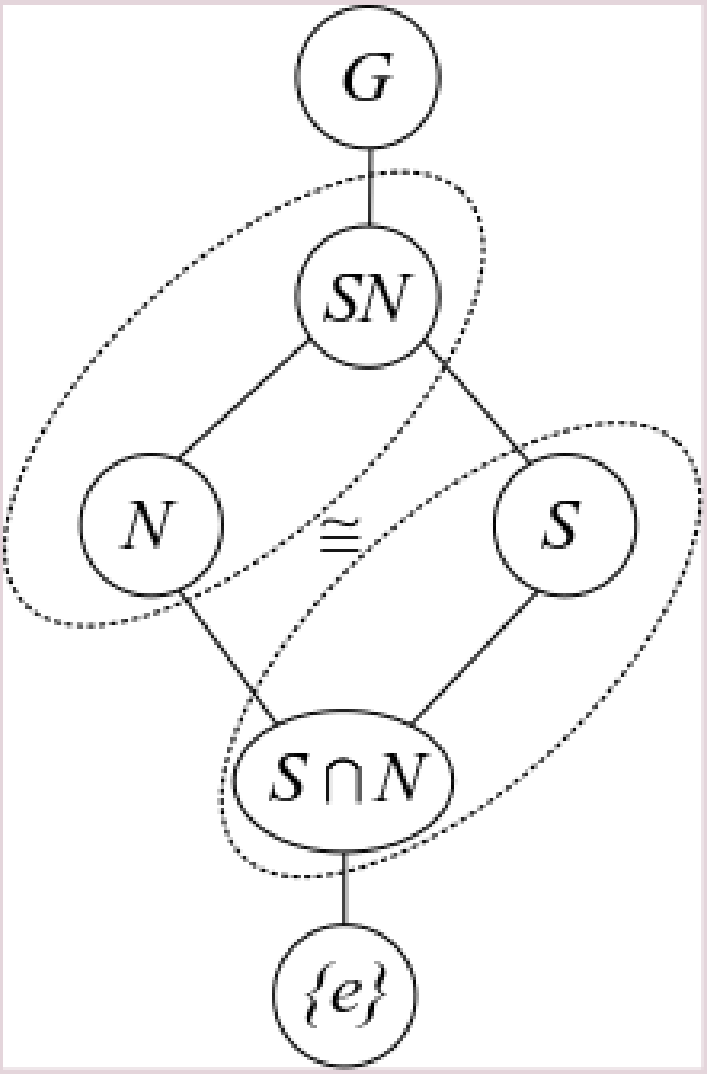


Figure 1: The 2nd "Diamond" Isomorphism Theorem

Remark 2.6.4: For this to make sense, we also have

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

If we relax the conditions to $S, N \leq G$ with $S \in N_G(N)$, then $S \cap N \trianglelefteq S$ (but is not normal in G) and the 2nd Isomorphism Theorem still holds.

Theorem 2.6.5 ***(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 $K \trianglelefteq G$ then $K/N \trianglelefteq G/N$.
3. Every subgroup of G/N is of the form K/N for some such $K \leq G$.
4. Every *normal* subgroup of G/N is of the form K/N for some such $K \trianglelefteq G$.
5. If $K \trianglelefteq G$, then we can cancel normal subgroups:

$$\frac{G/N}{K/N} \cong \frac{G}{K}.$$

Theorem 2.6.6 ***(The Correspondence Theorem / 4th Isomorphism Theorem).***
Suppose $N \trianglelefteq G$, then there exists a correspondence:

$$\left\{H < G \;\middle|\; N \subseteq H\right\} \rightleftharpoons \left\{H \;\middle|\; H < \frac{G}{N}\right\}$$
$$\left\{\begin{matrix}\text{Subgroups of } G \\ \text{containing } N\end{matrix}\right\} \rightleftharpoons \left\{\begin{matrix}\text{Subgroups of the} \\ \text{quotient } G/N\end{matrix}\right\}.$$

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

Fact 2.6.7
$N \trianglelefteq G$ and $N \subseteq H < G \implies N \trianglelefteq H$.

2.7 Products

Theorem 2.7.1 ***(Chinese Remainder Theorem).***

$$\gcd(p, q) = 1 \implies \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}.$$

Theorem 2.7.2 ***(Recognizing Direct Products).***
We have $G \cong H \times K$ when

- $H, K \trianglelefteq G$
- $G = HK$.

- $H \cap K = \{e\} \subset G$

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

Theorem 2.7.3 ***(Recognizing Generalized Direct Products).***
We have $G \cong \prod_{i=1}^{n} H_i$ when

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

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

Theorem 2.7.4 ***(Recognizing Semidirect Products).***
We have $G \cong N \rtimes_\psi H$ when

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

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

Relaxed condition: $H, N \trianglelefteq G$ for direct product, or just $H \leq G$ fo

Proposition 2.7.5.
If $H, K \leq G$ and $H \leq N_G(K)$ (or $K \trianglelefteq G$) then $HK \leq G$ is a subgroup.

2.8 Automorphism Groups

Fact 2.8.1

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

- $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(n)\mathbb{Z}$ where φ is the totient function.
  - $\varphi(p^k) = p^{k-1}(p-1)$
- If G, H have coprime order then $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

2.9 Sylow Theorems

Definition 2.9.1
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.

2.9.1 Sylow 1 (Cauchy for Prime Powers)

Theorem 2.9.2 ***(Sylow 1).***

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

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.

2.9.2 Sylow 2 (Sylows are Conjugate)

Theorem 2.9.3 ***(Sylow 2).***
All Sylow-p subgroups S_p are conjugate, i.e.

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

Corollary 2.9.4.

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

2.9.3 Sylow 3 (Numerical Constraints)

Theorem 2.9.5 ***(Sylow 3).***

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

Corollary 2.9.6.
p does not divide n_p.

Proposition 2.9.7.
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 $H \coloneqq \cup_i H^i$ is maximal and thus a Sylow p-subgroup.

■

2.10 Special Classes of Groups

Definition 2.10.1 (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 2.10.2 (p-groups)
If $|G| = p^k$, then G is a **p-group.**

Definition 2.10.3 (Normalizers Grow)
If for every proper $H < G$, $H \trianglelefteq N_G(H)$ is again proper, then "normalizers grow" in G.

2.11 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^2q: ?

2.11.1 Finitely Generated Abelian Groups

Definition 2.11.1 (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 → Elementary Divisors:

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

Example 2.11.2:

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

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 2.11.3: 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	$\varnothing$

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

$p=2$	$p=3$	$p=5$
2	$\varnothing$	$\varnothing$

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

and thus

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

2.11.2 Classifying Abelian Groups of a Given Order

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

Example 2.11.4 ***(?):*** Example: $p(6) = 11$, given by

$$\begin{aligned}
&[6],\\
&[5,1],\\
&[4,2],\\
&[4,1,1],\\
&[3,3],\\
&[3,2,1],\\
&[3,1,1,1],\\
&[2,2,2],\\
&[2,2,1,1],\\
&[2,1,1,1,1],\\
&[1,1,1,1,1,1].
\end{aligned}$$

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.

2.12 Series of Groups

Definition 2.12.1 (Normal Series)
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 2.12.2 (Central Series)
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 2.12.3 (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 2.12.4 ***(Jordan-Holder).***
Any two composition series of a group have the same length and isomorphic composition factors (up to permutation).

Definition 2.12.5 (Simple Groups)
A group G is **simple** iff $H \trianglelefteq G \implies H = \{e\}, G$, i.e. it has no non-trivial proper subgroups.

Proposition 2.12.6.
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 $N \to E \to G/N$.

Definition 2.12.7 (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 a
the map is nilpotent, so call G nilpotent!

Definition 2.12.8 (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 $\pi : G \to G/Z_i$, so define $Z_{i+1} \coloneqq \pi^{-1}(Z(G/Z_i))$ (?).

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

Definition 2.12.9 (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 2.12.10 (Solvable)
A group G is **solvable** iff G has a terminating normal series with abelian composition factors, i.e.

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

Theorem 2.12.11 ***(Characterization of Solvable).***
A group G is solvable iff its derived series terminates.

Theorem 2.12.12 ***(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.

3 | Ring Theory

3.1 Definitions

Notation:

- $\langle a \rangle \coloneqq Ra \coloneqq \left\{ ra \;\middle|\; r \in R \right\}$ is the ideal generated by a single element.

3.1.1 Undergrad Review

Definition 3.1.1 (Divisibility of Elements)
An element $r \in R$ is **divisible** by $q \in R$ if and only if there exists some $c \in R$ such that $r = qc$. In this case, we sometimes write $q \mid r$.

Definition 3.1.2 (Irreducible Element)
An element $r \in R$ is **irreducible** iff

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

Definition 3.1.3 (Prime Element)
An element $p \in R$ is **prime** iff

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

Definition 3.1.4 (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

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

fails to be injective.

Definition 3.1.5 (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 3.1.6 (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 $J_1, J_2 \supseteq I$ such that $J_1 \cap J_2 = I$.

Definition 3.1.7 (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 3.1.8 (Maximal Ideal)
$\mathfrak{m}$ is **maximal** $\iff (I \trianglelefteq R, I \neq R \implies I \subseteq \mathfrak{m}) \iff R/I$ is a field.

Definition 3.1.9 (Prime Spectrum)
The **prime spectrum** (or just the **spectrum**) of R is defined as

$$\operatorname{Spec}(R) = \left\{ \text{pr} \trianglelefteq R \;\middle|\; \text{pr is prime} \right\}.$$

Definition 3.1.10 (Max Spectrum)
The **max spectrum** of R is defined as

$$\operatorname{mSpec}(R) = \left\{ \mathfrak{m} \trianglelefteq R \;\middle|\; \mathfrak{m} \text{ is maximal} \right\}.$$

Definition 3.1.11 (Integral Domain)
A ring is an **integral domain** if and only if it has no nonzero zero divisors:

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

Definition 3.1.12 (Principal Ideal)
An ideal $I \trianglelefteq R$ if **principal** if there exists an $a \in R$ such that $I = \langle a \rangle$.

Definition 3.1.13 (Principal Ideal Domain)
A ring R is a **principal ideal domain** iff every ideal is principal.

Definition 3.1.14 (Unique Factorization Domain)
A ring R is a **unique factorization domain** 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.

3.1.2 Types of Rings

Definition 3.1.15 (Simple Modules)
A module M is **simple** iff every submodule $M' \leq M$ is either 0 or M. A ring R is simple if and only if it is simple as an R-module, i.e. there are no nontrivial proper ideals.

Definition 3.1.16 (Semisimple Modules)
A module M is **simple** if and only if it admits a decomposition

$$M = \bigoplus_{j \in J} M_j$$

with each M_j simple.

Definition 3.1.17 (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 $I_N = I_{N+1} = \cdots$.

3.1.3 Commutative Algebra

Definition 3.1.18 (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 3.1.19 (Nilradical)
$\mathfrak{N}(R) \coloneqq \left\{ x \in R \;\middle|\; x^n = 0 \text{ for some } n \right\}$ is the **nilradical** of R.

Definition 3.1.20 (Jacobson Radical)
The **Jacobson radical** $\mathfrak{J}(R)$ is the intersection of all maximal ideals, i.e.

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

Definition 3.1.21 (Reduced Ring)
A ring R is **reduced** if R contains no nonzero nilpotent elements.

Definition 3.1.22 (Local Ring)
A ring R is **local** iff it contains a unique maximal ideal.

Definition 3.1.23 (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 3.1.24 (Radical Ideal)
An ideal is **radical** iff $\operatorname{rad}(I) = I$.

3.2 Structure Theorems

Proposition 3.2.1 ***(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 3.2.2.
Fields $\subset$ Euclidean domains $\subset$ PIDs $\subset$ UFDs $\subset$ Integral Domains $\subset$ Rings

Example 3.2.3:

- 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*: $2 \pmod 4$ is a zero divisor.

Proposition 3.2.4.
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.

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

Proposition 3.2.5.
If R is a PID, then every element in R has a unique prime factorization.

Theorem 3.2.6 ***(Krull).***
Every ring has proper maximal ideals, and any proper ideal is contained in a maximal ideal.

Theorem 3.2.7 ***(Artin-Wedderburn?).***
If R is a nonzero, unital, *semisimple* ring then $R \cong \bigoplus_{i=1}^{m} \mathrm{Mat}(n_i, D_i)$, a finite sum of matrix rings over division rings.

Corollary 3.2.8.
If M is a simple ring over R a division ring, the M is isomorphic to a matrix ring.

3.3 Zorn's Lemma

Theorem 3.3.1 ***(Zorn's Lemma).***
If P is a poset in which every chain has an upper bound, then P has a maximal element.

Proposition 3.3.2.
Fields are simple rings.

Proposition 3.3.3.
If $I \trianglelefteq R$ is a proper ideal $\iff$ I contains no units.

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

Proposition 3.3.4.
If $I_1 \subseteq I_2 \subseteq \cdots$ are ideals then $\cup_j I_j$ is an ideal.

Proposition 3.3.5.
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 $\widehat{C} = \cup_i C_i$.
$\widehat{C}$ **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.

■

Example 3.3.6 ***(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.

Example 3.3.7: Maximal ideals of $R[x]$ are of the form $I = (x - a_i)$ for some $a_i \in R$.

4 | Fields

4.1 Definitions

Let k denote a field, and L/k extensions.

Definition 4.1.1 (Characterizations of Perfect Fields)
The following are equivalent:

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

Definition 4.1.2 (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.

Definition 4.1.3 (Prime Subfield)
The **prime subfield** of a field F is the subfield generated by 1.

Definition 4.1.4 (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 4.1.5 (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 4.1.6 (Separable Field Extension)
Let L/k be a field extension, $\alpha \in L$ be arbitrary, and $f(x) \coloneqq \min(\alpha, k)$. The following are equivalent

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

Definition 4.1.7 (Field Automorphisms)

$$\mathrm{Aut}(L/k) = \left\{ \sigma : L \to L \;\middle|\; \sigma|_k = \mathrm{id}_k \right\}.$$

Definition 4.1.8 (Galois Extension and Galois Group)
Let L/k be a finite field extension. The following are equivalent:

1. L/k is a **Galois extension**.
2. $|\mathrm{Aut}(L/k)| = [L : k]$
3. The fixed field of $\mathrm{Aut}(L/k)$ is exactly k.
4. L is the splitting field of a separable polynomial $p \in K[x]$.
5. L is finite, normal, and separable.

In this case, we define the **Galois group** as

$$\mathrm{Gal}(L/k) \coloneqq \mathrm{Aut}(L/k).$$

Definition 4.1.9 (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 $k < n$.

Definition 4.1.10 (Simple Extension)
An extension F/k is **simple** if $F = k[\alpha]$ for a single element α.

4.2 Facts

Fact 4.2.1

- 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 4.2.2 ***(Finite Extensions are Algebraic).***
Every finite extension is algebraic.

Proof .
If K/F and $[K : F] = n$, then pick any $\alpha \in K$ and consider $1, \alpha, \alpha^2, \ldots$. This yields $n + 1$ elements in an n-dimensional vector space, and thus there is a linear dependence

$$f(\alpha) \coloneqq \sum_{j=1}^{n} c_j \alpha^j = 0.$$

But then α is the root of the polynomial f.

■

Theorem 4.2.3 ***(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 4.2.4.
A primitive polynomial $p \in \mathbb{Q}[x]$ is irreducible $\iff p$ is irreducible in $\mathbb{Z}[x]$.

Theorem 4.2.5 ***(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 $\mathbb{Z}[x]$.

4.3 Finite Fields

Theorem 4.3.1 ***(Characterization of Prime Subfields).***
The prime subfield of any field is isomorphic to either $\mathbb{Q}$ or $\mathbb{F}_p$ for some p.

Proposition 4.3.2.
If $\operatorname{ch} k = p$ then $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$.

Proof .
Todo

■ Proof

Theorem 4.3.3 ***(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 4.3.4 ***(Prime Subfields of Finite Fields).***
Every finite field F is isomorphic to a unique field of the form $\mathbb{GF}(p^n)$ and if $\operatorname{ch} F = p$, it has prime subfield $\mathbb{F}_p$.

Proposition 4.3.5 ***(Containment of Finite Fields).***
$\mathbb{GF}(p^\ell) \leq \mathbb{GF}(p^k) \iff \ell$ divides k.

Proposition 4.3.6 ***(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.

■

Proposition 4.3.7 ***(Splits Product of Irreducibles).***
Let $\rho_n \coloneqq x^{p^n} - x$. Then $f(x) \mid \rho_n(x) \iff \deg f \mid n$ and f is irreducible.

Corollary 4.3.8.
$x^{p^n} - x = \prod f_i(x)$ 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 $f \mid x^{p^d} - x$, by considering $F[x]/\langle f \rangle$.
- Thus $x^{p^d} - x \mid x^{p^n} - x \iff d \mid n$.

$\Longrightarrow$:

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

■

Proposition 4.3.9.
No finite field is algebraically closed.

Proof .
If $k = \{a_1, a_2, \cdots a_n\}$ then define the polynomial

$$f(x) \coloneqq 1 + \prod_{j=1}^{n} (x - a_j) \in k[x].$$

This has no roots in k.

■ Proof

4.4 Galois Theory

Proposition 4.4.1.
If $\operatorname{ch} k = 0$ or k is finite, then every *algebraic* extension L/k is separable.

Proposition 4.4.2.
If L/k is algebraic, then $\operatorname{Aut}(L/k)$ permutes the roots of irreducible polynomials.

Proposition 4.4.3.
$|\operatorname{Aut}(L/k)| \leq [L : k]$ with equality precisely when L/k is normal.

4.4.1 Lemmas About Towers

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

Proposition 4.4.4 ***(Towers are multiplicative in degree).***

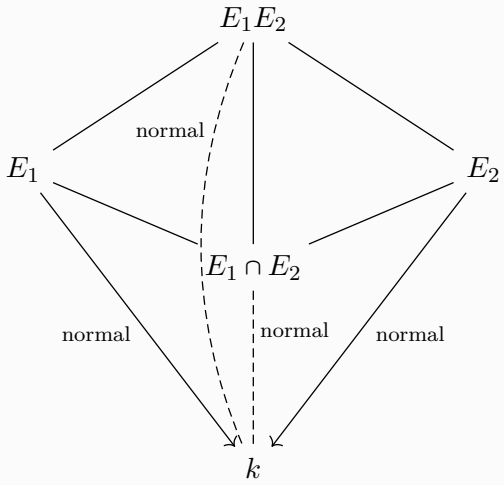
$$[L : k] = [L : F][F : k].$$

Proposition 4.4.5 ***(Normal/Algebraic/Galois in towers).***
L/k normal/algebraic/Galois $\implies$ L/F normal/algebraic/Galois.

Proof (for normality).
$\min(\alpha, F) \mid \min(\alpha, k)$, so if the latter splits in L then so does the former.
■

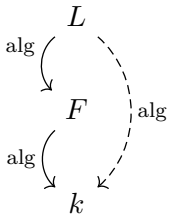
Corollary 4.4.6 ***(?).***
$\alpha \in L$ algebraic over k $\implies$ α algebraic over F.

Corollary 4.4.7 ***(?).***
E_1/k normal and E_2/k normal $\implies$ E_1E_2/k normal and $E_1 \cap E_2/k$ normal.

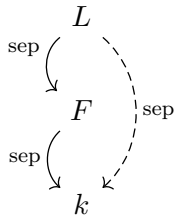


Link to diagram

Proposition 4.4.8 ***(Algebraicity is transitive).***
F/k algebraic and L/F algebraic $\implies$ L/k algebraic.

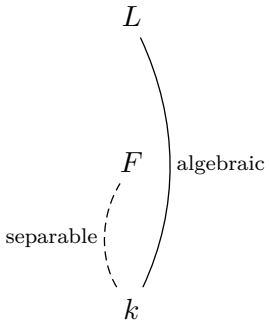


Proposition 4.4.9 ***(Separability is transitive).***
For $L/F/k$, then L/k is separable $\iff$ L/F, F/k are separable.



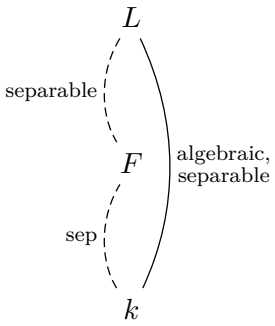
⚠ **Warning 4.4.10**
Being Galois is **not** transitive. Take $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$.

Proposition 4.4.11 *(?).*
If L/k is algebraic, then F/k separable:



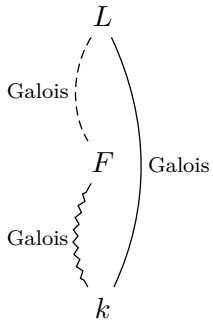
Link to diagram

Moreover, L/F is additionally separable $\iff$ L/k separable:



Link to diagram

Proposition 4.4.12 *(?).*
If L/k is Galois, then L/F is **always** Galois. Moreover, F/k is Galois if and only if $\mathrm{Gal}(L/F) \trianglelefteq \mathrm{Gal}(L/k)$



Link to diagram

In this case,

$$\mathrm{Gal}(F/k) \cong \frac{\mathrm{Gal}(L/k)}{\mathrm{Gal}(L/F)}.$$

4.4.2 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.

4.5 Fundamental Theorem of Galois Theory

Theorem 4.5.1 ***(Fundamental Theorem of Galois Theory).***
Let L/k be a Galois extension, then there is a correspondence:

$$\begin{aligned}\left\{\text{Subgroups } H \leq \text{Gal}(L/k)\right\} &\rightleftharpoons \left\{\begin{smallmatrix}\text{Fields } F \text{ such} \\ \text{that } L/F/k\end{smallmatrix}\right\} \\ H &\to \left\{E^H \coloneqq \text{ The fixed field of } H\right\} \\ \left\{\text{Gal}(L/F) \coloneqq \left\{\sigma \in \text{Gal}(L/k) \;\middle|\; \sigma(F) = F\right\}\right\} &\leftarrow F\end{aligned}$$

- This is contravariant with respect to subgroups/subfields.
- $[F : k] = [G : H]$, so degrees of extensions over the base field correspond to indices of subgroups.
- $[K : F] = |H|$
- L/F is Galois and $Gal(K/F) = H$
- F/k is Galois $\iff$ H is normal, and $\text{Gal}(F/k) = \text{Gal}(L/k)/H$.
- The compositum F_1F_2 corresponds to $H_1 \cap H_2$.
- The subfield $F_1 \cap F_2$ corresponds to H_1H_2.

4.5.1 Examples

Example 4.5.2 ***(?):*** $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/(n)^\times$ and is generated by maps of the form $\zeta_n \mapsto \zeta_n^j$ where $(j, n) = 1$. I.e., the following map is an isomorphism:

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

Example 4.5.3 ***(?):*** $\text{Gal}(\mathbb{GF}(p^n)/\mathbb{F}_p) \cong \mathbb{Z}/(n)$, a cyclic group generated by powers of the Frobenius automorphism:

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

Proposition 4.5.4.
Every quadratic extension is Galois.

Proposition 4.5.5.
If K is the splitting field of an irreducible polynomial of degree n, then $\text{Gal}(K/\mathbb{Q}) \leq S_n$ is a transitive subgroup.

Corollary 4.5.6.
n divides the order $|\text{Gal}(K/\mathbb{Q})|$.

Theorem 4.5.7 ***(Splitting + Perfect implies Galois).***

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

Proposition 4.5.8 ***(Composite Extensions).***
If F/k is finite and Galois and L/k is arbitrary, then FL/L is Galois and

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

4.6 Cyclotomic Polynomials

Proposition 4.6.1.
$\deg \Phi_n(x) = \varphi(n)$ 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.

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

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 4.6.2.

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

Proposition 4.6.3.

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

Theorem 4.6.4 ***(Primitive Element).***
Every finite separable extension is simple.

Corollary 4.6.5.
$\mathbb{GF}(p^n)$ is a simple extension over $\mathbb{F}_p$.

5 Modules

5.1 General Modules

Definition 5.1.1 (Simple Module)
A module is **simple** iff it has no nontrivial proper submodules.

Definition 5.1.2 (Free Module)
A **free** module is a module with a basis (i.e. a spanning, linearly independent set).

Definition 5.1.3 (Torsionfree)
A module M is **torsion-free** if and only if for every $x \in M$, $mx = 0_M \implies m = 0_M$. I.e. the only torsion element of M is zero itself.

Fact 5.1.4
Free $\implies$ torsionfree.

Example 5.1.5 ***(?):*** $\mathbb{Z}/(6)$ is a $\mathbb{Z}$-module that is *not* free, since the element $[3]$ is a torsion element, where $2[3] = [6] = [0]$.

Definition 5.1.6 (Projective Modules)
A module M is **projective** iff M is a direct summand of a free module $F = M \oplus \cdots$.

Example 5.1.7 *(?):* Free implies projective, but not the converse. Let R_1, R_2 be two nontrivial rings and set $R \coloneqq R_1 \oplus R_2$. Then R_1, R_2 are projective R-modules by construction, but each factor contains R-torsion: setting $e \coloneqq (0,1) \in R$ we have $e \curvearrowright R_1 = 0_{R_1}$. Since free implies torsionfree, R_1 can not be a free R-module.

Definition 5.1.8 (Exact Sequences)
A sequence of R-module morphisms $0 \xrightarrow{d_1} A \xrightarrow{d_2} B \xrightarrow{d_3} C \to 0$ is *exact* iff $\operatorname{im} d_i = \ker d_{i+1}$.

Proposition 5.1.9 ***(Splitting Exact Seueqnces).***
If $0 \to A \to B \to C \to 0$ 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 5.2.1 ***(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.
$\Longleftarrow$: 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 6.0.1 (Invariant Factor)
Todo
todo

Definition 6.0.2 (Elementary Divisor)
Todo
todo

6.1 Minimal / Characteristic Polynomials

Fix some notation:

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

Definition 6.1.1 (?)
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 6.1.2 (?)
The **characteristic polynomial** of A is given by

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

Fact 6.1.3
If A is upper triangular, then $\det(A) = \prod_i a_{ii}$

Theorem 6.1.4 ***(Cayley-Hamilton).***
The minimal polynomial divides the characteristic polynomial, and in particular $\chi_A(A) = 0$.

Proof (?).
By minimality, $\min_A$ divides χ_A. Every λ_i is a root of $\min_A(x)$: 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 6.1.5 (Similar Matrices)
Two matrices A, B are **similar** (i.e. $A = PBP^{-1}$) $\iff$ A, B have the same Jordan Canonical Form (JCF).

Definition 6.1.6 (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 6.2.1 (Companion Matrix)
Given a monic $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + x^n$, the **companion matrix** of p is given

by

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

6.3 Canonical Forms

6.3.1 Rational Canonical Form

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

Theorem 6.3.1 ***(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 6.3.2 ***(RCG 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 $V \to F[x]$ 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.

■

6.3.2 Jordan Canonical Form

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

Lemma 6.3.3 ***(?).***
The elementary divisors of A are the minimal polynomials of the Jordan blocks.

Lemma 6.3.4 ***(JCF from Minimal and Characteristic Polynomials).***
Writing $\text{Spec}(A) = \{(\lambda_i, b_i)\}$,

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

- 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 6.4.1 ***(?).***
The characteristic polynomial is the *product of the invariant factors*, i.e.

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

Lemma 6.4.2 ***(?).***
The minimal polynomial of A is the *invariant factor of highest degree*, i.e.

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

Proposition 6.4.3 ***(?).***
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 6.5.1 *(?).*
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 6.5.2 ***(The Spectral Theorem).***

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

Proof (?).

- Suppose A is Hermitian.
- Since V itself is an invariant subspace, A has an eigenvector $\mathbf{v}_1 \in V$.
- Let $W_1 = \operatorname{span}_k \{\mathbf{v}_1\} \perp$.
- 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 6.5.3 ***(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 6.5.4 ***(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

Example 6.6.1 ***(?):*** 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 $\mathbb{C}$
- $\min_M(x) = \chi_M(x) = x^2 + 1$

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

Example 6.6.2 *(?):* A matrix that:

- Is not diagonalizable over $\mathbb{C}$,
- Has eigenvalues $[1, 1]$ (repeated, multiplicity 2)
- $\min_M(x) = \chi_M(x) = x^2 - 2x + 1$

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

Example 6.6.3 *(?):* Non-similar matrices with the same characteristic polynomial

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

Example 6.6.4 *(?):* A full-rank matrix that is not diagonalizable:

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

Example 6.6.5 *(?):* Matrix roots of unity:

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

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

7 | Extra Problems

7.1 Commutative Algebra

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

7.2 Group Theory

7.2.1 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 $H \cap K = \varnothing$, 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 $|G|/|H| = [G : H]$.

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

Conjugacy

- Show that the size of a conjugacy class divides the order of a group.

- Let G be finite with $H \leq G$ and show that G is not the union of the conjugates of H.

Hint: consider the intersection and count.

Hint: Orbit-stabilizer

7.2.2 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 $H \leq G$, $C_H(x) = H \cap C_G(x)$.
- Let $H, K \leq G$ a finite group, and without using the normalizers of H or K, show that $|HK| = |H||K|/|H \cap K|$.
- 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.

7.2.3 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 –

  - 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

- 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.
- Let p be a prime and $|G| = p^3$. Prove that G has a normal subgroup N of order p^2.
  - Suppose $N = \langle h \rangle$ is cyclic and classify all possibilities for G if:
    - $|h| = p^3$
    - $|h| = p$.

Hint: Sylow and semidirect products.

- Show that any normal p- subgroup is contained in every Sylow p-subgroup of G.
- Show that the order of $1 + p$ in $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ is equal to p. Use this to construct a non-abelian group of order p^3.

7.2.4 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 $P \cap H \in \mathrm{Syl}_p(H)$.
- Show that Sylow p_i-subgroups S_{p_1}, S_{p_2} for distinct primes $p_1 \neq p_2$ intersect trivially.
- Show that in a p group, every normal subgroup intersects the center nontrivially.

7.2.5 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.

7.2.6 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.

7.2.7 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.

7.2.8 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.

7.2.9 Classification

- Show that no group of order 36 is simple.
- Show that no group of order 90 is simple.
- Classifying all groups of order 99.
- 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 $G \cong A_4$.
- Suppose $|G| = 240 = s^4 \cdot 3 \cdot 5$.
  - How many Sylow-p subgroups does G have for $p \in \{2, 3, 5\}$?
  - Show that if G has a subgroup of order 15, it has an element of order 15.
  - Show that if G does not have such a subgroup, the number of Sylow-3 subgroups is either 10 or 40.

Hint: Sylow on the subgroup of order 15 and semidirect pro

7.2.10 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.

7.2.11 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

7.2.12 Misc

- Prove Burnside's theorem.
- Show that $\text{Inn}(G) \trianglelefteq Aut(G)$
- Show that $\text{Inn}(G) \cong G/Z(G)$
- Show that the kernel of the map $G \to \text{Aut}(G)$ 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.

7.2.13 Nonstandard Topics

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

Thus "characteristic" is a strictly stronger condition than n

- 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 "ch tivity.

8

8.1 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

Problem. (Units or Zero Divisors)
Every $a \in R$ for a finite ring is either a unit or a zero divisor.

Solution:

- 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.

Problem. (Maximal implies prime)
Maximal $\implies$ prime, but generally not the converse.

Solution:

- 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.

- 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 $\cup_{\mathfrak{m}\in \text{maxSpec}(R)} = R \setminus R^\times$.
- Show that $\text{maxSpec}(R) \subsetneq \text{Spec}(R)$ but the containment is strict.
- $\star$ Show that if x is not a unit, then x is contained in some maximal ideal.
- Show that every prime ideal is radical.
- Show that the nilradical is given by $\mathfrak{N}(R) = \text{rad}(0)$.
- Show that $\text{rad}(IJ) = \text{rad}(I) \cap \text{rad}(J)$
- Show that if $\text{Spec}(R) \subseteq \text{maxSpec}(R)$ then R is a UFD.
- Show that if R is Noetherian then every ideal is finitely generated.

Characterizing Certain Ideals

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

Problem. (Jacobson radical is bigger than the nilradical)
The nilradical is contained in the Jacobson radical, i.e.

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

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

Problem. (Mod by nilradical to kill nilpotents)
$R/\mathfrak{N}(R)$ has no nonzero nilpotent elements.

Solution:

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

Problem. (Nilradical is intersection of primes)
The nilradical is the intersection of all prime ideals, i.e.

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

Solution: • $\mathfrak{N} \subseteq \cap \mathfrak{p}$:

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

- $\mathfrak{N}^c \subseteq \cup \mathfrak{p}^c$:
- 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.

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

8.2 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.

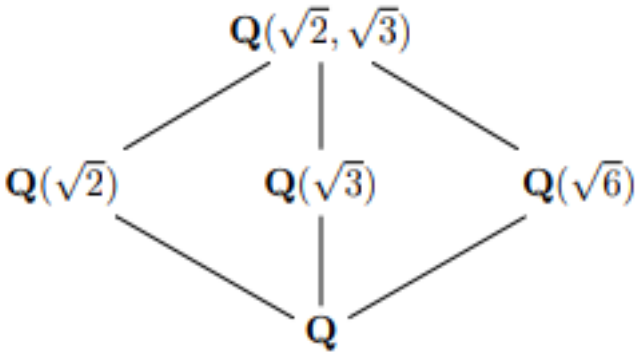
8.3 Galois Theory

8.3.1 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 $\mathrm{ch}(F) \neq 2$ 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 $E \cap F = k$, then EF/k is Galois and $G(EF/k) \cong G(E/k) \times G(F/k)$.

8.3.2 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.

8.4 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 $T : V \to V$ 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 $T(\mathbf{v}_i) = \mathbf{v}_{i+1 \pmod n}$ 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.

8.5 Linear Algebra

Sort out from module section.

9 Even More Algebra Question (In Progress)

9.1 Groups

9.1.1 Question 1.1

What is a normal subgroup? Can you get some natural map from a normal subgroup? What topological objects can the original group, normal subgroup, and quotient group relate to?

9.1.2 Question 1.2

Prove that a subgroup of index two is normal.

9.1.3 Question 1.3

Find all normal subgroups of A_4.

9.1.4 Question 1.4

Give an interesting example of a non-normal subgroup. Is SO(2) normal inside $SL_2(R)$?

9.1.5 Question 1.5

Is normality transitive? That is, is a normal subgroup of a normal subgroup normal in the biggest group?

9.1.6 Question 1.6.

Define a solvable group. Give an example of a solvable nonabelian group.

Show A_4 is solvable. Do the Sylow theorems tell you anything about whether this index 3 subgroup of A_4 is normal?

9.1.7 Question 1.7

Define lower central series, upper central series, nilpotent and solvable groups.

9.1.8 Question 1.8

Define the derived series. Define the commutator. State and prove two nontrivial theorems about derived series.

9.1.9 Question 1.9

Prove that $SL_2(Z)$ is not solvable.

9.1.10 Question 1.10

What are all possible orders of elements of $\mathrm{SL}_2(Z)$?

9.1.11 Question 1.11

Can you show that all groups of order p^n for p prime are solvable? Do you know how to do this for groups of order $p^r q^s$?

9.1.12 Question 1.12

Suppose a p-group acts on a set whose cardinality is not divisible by p (p prime). Prove that there is a fixed point for the action.

9.1.13 Question 1.13

Prove that the centre of a group of order pr (p prime) is not trivial.

9.1.14 Question 1.14

Give examples of simple groups. Are there infinitely many?

9.1.15 Question 1.15

State and prove the Jordan-Holder theorem for finite groups.

9.1.16 Question 1.16

What's Cayley's theorem? Give an example of a group of order n that embeds in S_m for some m smaller than n.

Give an example of a group where you have to use S_n.

9.1.17 Question 1.17

Is A_4 a simple group? What are the conjugacy classes in S_4? What about in A_4?

9.1.18 Question 1.18

Talk about conjugacy classes in the symmetric group S_n.

9.1.19 Question 1.19

When do conjugacy classes in S_n split in A_n?

9.1.20 Question 1.20

What is the centre of S_n? Prove it.

9.1.21 Question 1.21

Prove that the alternating group A_n is simple for $n \geq 5$.

9.1.22 Question 1.22

Prove the alternating group on n letters is generated by the 3-cycles for $n \geq 3$.

9.1.23 Question 1.23

Prove that for p prime, Sp is generated by a p-cycle and a transposition.

9.1.24 Question 1.24

What is the symmetry group of a tetrahedron? Cube? Icosahedron?

9.1.25 Question 1.25

How many ways can you color the tetrahedron with C colors if we identify symmetric colorings?

9.1.26 Question 1.26.

What is the symmetry group of an icosahedron? What's the stabiliser of an edge?

How many edges are there? How do you know the symmetry group of the icosahedron is the same as the symmetry group of the dodecahedron?

Do you know the classification of higher-dimensional polyhedra?

9.1.27 Question 1.27

Do you know what the quaternion group is? How many elements are there of each order?

9.1.28 Question 1.28

What is the group of unit quaternions topologically? What does it have to do with SO(3)?

9.1.29 Question 1.29

What's the stabiliser of a point in the unit disk under the group of conformal automorphisms?

9.1.30 Question 1.30

What group-theoretic construct relates the stabiliser of two points?

9.1.31 Question 1.31

Consider $\mathrm{SL}_2(R)$ acting on $\mathbb{R}^2$ by matrix multiplication. What is the stabiliser of a point? Does it depend which point? Do you know what sort of subgroup this is? What if $\mathrm{SL}_2(R)$ acts by Möbius transformations instead?

9.1.32 Question 1.32

What are the polynomials in two real variables that are invariant under the action of D_4, the symmetry group of a square, by rotations and reflections on the plane that the two variables form?

9.1.33 Question 1.33

Give an interesting example of a subgroup of the additive group of the rationals.

9.1.34 Question 1.34

Talk about the isomorphism classes of subgroups of $\mathbb{Q}$. How many are there? Are the ones you've given involving denominators divisible only by certain primes distinct? So that gives you the cardinality. Are these all of them?

9.1.35 Question 1.35

Is the additive group of the reals isomorphic to the multiplicative group of the positive reals? Is the same result true with reals replaced by rationals?

9.1.36 Question 1.36

What groups have nontrivial automorphisms?

9.1.37 Question 1.37

A subgroup H of a group G that meets every conjugacy class is in fact G. Why is that true?

9.1.38 Question 1.38

Let G be the group of invertible 3×3 matrices over $\mathbb{F}_p$, for p prime. What does basic group theory tell us about G?

How many conjugates does a Sylow p-subgroup have? Give a matrix form for the elements in this subgroup.

Explain the conjugacy in terms of eigenvalues and eigenvectors. give a matrix form for the normaliser of the Sylow p-subgroup.

9.1.39 Question 1.39

Let's look at $\mathrm{SL}_2(\mathbb{F}_3)$. How many elements are in that group? What is its centre? Identify $\mathrm{PSL}_2(\mathbb{F}_3)$ as a permutation group.

9.1.40 Question 1.40

How many elements does $\mathrm{GL}_2(\mathbb{F}_q)$ have? How would you construct representations?

What can you say about the 1-dimensional representations? What can you say about simplicity of some related groups?

9.1.41 Question 1.41.

A subgroup of a finitely-generated free abelian group is?

A subgroup of a finitely-generated free group is..? Prove your answers.

9.1.42 Question 1.42

Missing.

9.1.43 Question 1.43

What are the subgroups of the free group F_2? How many generators can you have?

Can you find one with 3 generators? 4 generators? Countably many generators?

Is the subgroup with 4 generators you found normal? Why? Can you find a normal one?

9.1.44 Question 1.44

Talk about the possible subgroups of $\mathbb{Z}^3$. Now suppose that you have a subgroup of $\mathbb{Z}^3$. What theorem tells you something about the structure of the quotient group?

9.2 Classification of Finite groups

9.2.1 Question 2.1

Given a finite abelian group with at most n elements of order divisible by n, prove it's cyclic.

9.2.2 Question 2.2

Suppose I asked you to classify groups of order 4. Why isn't there anything else? Which of those could be realised as a Galois group over $\mathbb{Q}$?

9.2.3 Question 2.3

State/prove the Sylow theorems.

9.2.4 Question 2.4

Classify groups of order 35.

9.2.5 Question 2.5

Classify groups of order 21.

9.2.6 Question 2.6

Discuss groups of order 55.

9.2.7 Question 2.7

Classify groups of order 14. Why is there a group of order 7? Are all index-2 subgroups normal?

9.2.8 Question 2.8

How many groups are there of order 15? Prove it.

9.2.9 Question 2.9

Classify all groups of order 8.

9.2.10 Question 2.10

Classify all groups of order p^3 for p prime.

9.2.11 Question 2.11

What are the groups of order p^2? What about pq? What if q is congruent to 1 $(\text{mod } p)$?

9.2.12 Question 2.12

What are the groups of order 12? Can there be a group of order 12 with 2 nonisomorphic subgroups of the same order?

9.2.13 Question 2.13

How would you start finding the groups of order 56? Is there in fact a way for $\mathbb{Z}/7\mathbb{Z}$ to act on a group of order 8 nontrivially?

9.2.14 Question 2.14

How many abelian groups are there of order 36?

9.2.15 Question 2.15

What are the abelian groups of order 16?

9.2.16 Question 2.16.

What are the abelian groups of order 9? Prove that they are not isomorphic. groups of order 27?

9.2.17 Question 2.17

How many abelian groups of order 200 are there?

9.2.18 Question 2.18

Prove there is no simple group of order 132.

9.2.19 Question 2.19

Prove that there is no simple group of order 160. What can you say about the structure of groups of that order?

9.2.20 Question 2.20

Prove that there is no simple group of order 40.

9.3 Fields and Galois Theory

9.3.1 Question 3.1

What is the Galois group of a finite field? What is a generator? How many elements does a finite field have? What can you say about the multiplicative group? Prove it.

9.3.2 Question 3.2

Classify finite fields, their subfields, and their field extensions. What are the automorphisms of a finite field?

9.3.3 Question 3.3

Take a finite field extension $\mathbb{F}_p^n$ over $\mathbb{F}_p$. What is Frobenius? What is its characteristic polynomial?

9.3.4 Question 3.4

What are the characteristic and minimal polynomial of the Frobenius automorphism?

9.3.5 Question 3.5

What's the field with 25 elements?

9.3.6 Question 3.6

What is the multiplicative group of $\mathbb{F}_9$?

9.3.7 Question 3.7

What is a separable extension? Can $\mathbb{Q}$ have a non-separable extension? How about $\mathbb{Z}/p\mathbb{Z}$? Why not? Are all extensions of characteristic 0 fields separable? Of finite fields? Prove it.

Give an example of a field extension that's not separable.

9.3.8 Question 3.8

Are there separable polynomials of any degree over any field?

9.3.9 Question 3.9

What is a perfect field and why is this important? Give an example of a non-perfect field.

9.3.10 Question 3.10

What is Galois theory? State the main theorem. What is the splitting field of $x^5 - 2$ over $\mathbb{Q}$? What are the intermediate extensions? Which extensions are normal, which are not, and why? What are the Galois groups (over Q) of all intermediate extensions?

9.3.11 Question 3.11

What is a Galois extension?

9.3.12 Question 3.12

Take a quadratic extension of a field of characteristic 0. Is it Galois? Take a degree 2 extension on top of that. Does it have to be Galois over the base field? What statement in group theory can you think of that reflects this?

9.3.13 Question 3.13.

Is Abelian Galois extension transitive? That is, if K has abelian Galois group over E, E has abelian Galois group over F , and K is a Galois extension of F, is it necessarily true that $\mathrm{Gal}(K/F)$ is also abelian? Give a counterexample involving number fields as well as one involving function fields.

9.3.14 Question 3.14

What is a Kummer extension?

9.3.15 Question 3.15

Say you have a field extension with only finitely many intermediate fields. Show that it is a simple extension.

9.3.16 Question 3.16

Tell me a condition on the Galois group which is implied by irreducibility of the polynomial. What happens when the polynomial has a root in the base field?

9.3.17 Question 3.17

What is the discriminant of a polynomial?

9.3.18 Question 3.18

If we think of the Galois group of a polynomial as contained in S_n, when is it contained in A_n?

9.3.19 Question 3.19

Is $\mathbb{Q}(\sqrt[3]{21})$ normal? What is its splitting field? What is its Galois group? Draw the lattice of subfields.

9.3.20 Question 3.20

What's the Galois group of $x^2 + 1$ over Q? What's the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$?

9.3.21 Question 3.21

What's the Galois group of $x^2 + 9$?

9.3.22 Question 3.22

What is the Galois group of $x^2 - 2$? Why is $x^2 - 2$ irreducible?

9.3.23 Question 3.23

Missing

9.3.24 Question 3.24

Missing

9.3.25 Question 3.25

What are the Galois groups of irreducible cubics?

Missing

9.3.26 Question 3.26

If an irreducible cubic polynomial has Galois group NOT contained in A3, does it necessarily have to be all of S_3?

9.3.27 Question 3.27

Compute the Galois group of $x^3 - 2$ over the rationals.

9.3.28 Question 3.28

How would you find the Galois group of $x^3 + 2x + 1$? Adjoin a root to $\mathbb{Q}$. Can you say something about the roots of $x^3 + 3x + 1$ in this extension?

9.3.29 Question 3.29

Compute the Galois group of $x^3 + 6x + 3$.

9.3.30 Question 3.30

Find the Galois group of $x^4 - 2$ over Q.

9.3.31 Question 3.31

What's the Galois group of $x^4 - 3$?

9.3.32 Question 3.32

What is the Galois group of $x^4 - 2x^2 + 9$?

9.3.33 Question 3.33

Calculate the Galois group of $x^5 - 2$.

9.3.34 Question 3.34.

Discuss sufficient conditions on a polynomial of degree 5 to have Galois group S_5 over $\mathbb{Q}$ and prove your statements.

9.3.35 Question 3.35

Show that if f is an irreducible quintic with precisely two non-real roots, then its Galois group is S_5.

9.3.36 Question 3.36

Suppose you have a degree 5 polynomial over a field. What are necessary and sufficient conditions for its Galois group to be of order divisible by 3? Can you give an example of an irreducible polynomial in which this is not the case?

9.3.37 Question 3.37

What is the Galois group of $x^7 - 1$ over the rationals?

9.3.38 Question 3.38

What is the Galois group of the polynomial $x^n - 1$ over $\mathbb{Q}$?

9.3.39 Question 3.39

Describe the Galois theory of cyclotomic extensions.

9.3.40 Question 3.40

What is the maximal real field in a cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$?

9.3.41 Question 3.41

Compute the Galois group of $p(x) = x^7 - 3$.

9.3.42 Question 3.42

What Galois stuff can you say about $x^{2n} - 2$?

9.3.43 Question 3.43

What are the cyclic extensions of (prime) order p?

9.3.44 Question 3.44

Can you give me a polynomial whose Galois group is $\mathbb{Z}/3\mathbb{Z}$?

9.3.45 Question 3.45

Which groups of order 4 can be realised as a Galois group over $\mathbb{Q}$?

9.3.46 Question 3.46

Give a polynomial with S_3 as its Galois group.

9.3.47 Question 3.47

Give an example of a cubic with Galois group S_3.

9.3.48 Question 3.48

How do you construct a polynomial over $\mathbb{Q}$ whose Galois group is S_n? Do it for $n = 7$ in particular.

9.3.49 Question 3.49

What's a Galois group that's not S_n or A_n?

9.3.50 Question 3.50

Which finite groups are Galois groups for some field extension?

9.3.51 Question 3.51

What Galois group would you expect a cubic to have?

9.3.52 Question 3.52

Draw the subgroup lattice for S_3.

9.3.53 Question 3.53

Do you know what the quaternion group is? How many elements are there of each order? Suppose I have a field extension of the rationals with Galois group the quaternion group. How many quadratic extensions does it contain? Can any of them be imaginary?

9.3.54 Question 3.54

Suppose you are given a finite Galois extension $K/\mathbb{Q}$ by $f(x) \in \mathbb{Z}[x]$ such that $\deg(f) = n$ and $\mathrm{Gal}(K/Q) = S_n$. What can you say about the roots?

9.3.55 Question 3.55

How many automorphisms does the complex field have? How can you extend the automorphisms of an algebraic field into $\mathbb{C}$? How can you extend a simple automorphism (e.g. a general subfield isomorphism? What feature of $\mathbb{C}$ allows you to?

Missing

9.3.56 Question 3.56.

Can it happen that a proper subfield of C is isomorphic to C? How?

9.3.57 Question 3.57

Consider the minimal polynomial $f(x)$ for a primitive mth root of unity. Prove that if p divides $f(a)$ for some integer a and $\gcd(p, m) = 1$ then m divides $p - 1$. Use this fact to show that there are infinitely many primes congruent to 1 $(\mathrm{mod}\ m)$.

9.3.58 Question 3.58

What is Dirichlet's theorem about primes in arithmetic progression? What can you say about the density of such primes?

9.3.59 Question 3.59

How many irreducible polynomials of degree six are there over $\mathbb{F}_2$?

9.3.60 Question 3.60

Can you have a degree 7 irreducible polynomial over $\mathbb{F}_p$? How about a degree 14 irreducible polynomial?

9.3.61 Question 3.61

How many irreducible polynomials are there of degree 4 over $\mathbb{F}_2$?

9.3.62 Question 3.62

For each prime p, give a polynomial of degree p that is irreducible over $\mathbb{F}_p$. You can do it in a "uniform" way.

9.3.63 Question 3.63

Can we solve general quadratic equations by radicals? And what about cubics and so on? Why can't you solve 5th degree equations by radicals?

9.3.64 Question 3.64

Talk about solvability by radicals. Why is S_5 not solvable? Why is A_5 simple?

9.3.65 Question 3.65

For which n can a regular n-gon be constructed by ruler and compass?

9.3.66 Question 3.66

How do you use Galois theory (or just field theory) to prove the impossibility of trisecting an angle? Doubling a cube? Squaring a circle?

9.3.67 Question 3.67

Which numbers are constructible? Give an example of a non-constructible number whose degree is nevertheless a power of 2.

9.3.68 Question 3.68

State and prove Eisenstein's Criterion.

9.3.69 Question 3.69

Why is $(x^p - 1)/(x - 1)$ irreducible over $\mathbb{Q}$?

9.3.70 Question 3.70

Can you prove the fundamental theorem of algebra using Galois theory? What do you need from analysis to do so?

9.3.71 Question 3.71

What are the symmetric polynomials?

9.3.72 Question 3.72

State the fundamental theorem of symmetric polynomials.

9.3.73 Question 3.73

Is the discriminant of a polynomial always a polynomial in the coefficients? What does this have to do with symmetric polynomials?

9.3.74 Question 3.74

Find a non-symmetric polynomial whose square is symmetric.

9.3.75 Question 3.75

Let f be a degree 4 polynomial with integer coefficients. What's the smallest finite field in which f necessarily has four roots?

9.3.76 Question 3.76

Define p-adic numbers. What is a valuation?

9.3.77 Question 3.77

What's Hilbert's theorem 90?

9.3.78 Question 3.78

Consider a nonconstant function between two compact Riemann Surfaces. How is it related to Galois theory?

9.4 Normal Forms

9.4.1 Question 4.1

What is the connection between the structure theorem for modules over a PID and conjugacy classes in the general linear group over a field?

9.4.2 Question 4.2

Explain how the structure theorem for finitely-generated modules over a PID applies to a linear operator on a finite dimensional vector space.

9.4.3 Question 4.3

I give you two matrices over a field. How would you tell if they are conjugate or not? What theorem are you using? State it. How does it apply to this situation? Why is $k[x]$ a PID? If two matrices are conjugate over the algebraic closure of a field, does that mean that they are conjugate over the base field too?

9.4.4 Question 4.4

If two real matrices are conjugate in $\mathrm{Mat}(n \times n, \mathbb{C})$, are they necessarily conjugate in $\mathrm{Mat}(n \times N, R)$ as well?

9.4.5 Question 4.5

Give the 4×4 Jordan forms with minimal polynomial $(x-1)(x-2)^2$.

9.4.6 Question 4.6

Talk about Jordan canonical form. What happens when the field is not algebraically closed?

9.4.7 Question 4.7

What are all the matrices that commute with a given Jordan block?

9.4.8 Question 4.8

How do you determine the number and sizes of the blocks for Jordan canonical form?

9.4.9 Question 4.9

For any matrix A over the complex numbers, can you solve $B^2 = A$?

9.4.10 Question 4.10

What is rational canonical form?

9.4.11 Question 4.11

Describe all the conjugacy classes of 3×3 matrices with rational entries which satisfy the equation $A^4 - A^3 - A + 1 = 0$. Give a representative in each class.

9.4.12 Question 4.12

What 3×3 matrices over the rationals (up to similarity) satisfy $f(A) = 0$, where $f(x) = (x^2+2)(x-1)^3$? List all possible rational forms.

Check

9.4.13 Question 4.13

What can you say about matrices that satisfy a given polynomial (over an algebraically closed field)? How many of them are there? What about over a finite field? How many such matrices are there then?

9.4.14 Question 4.14

What is a nilpotent matrix?

9.4.15 Question 4.15

When do the powers of a matrix tend to zero?

9.4.16 Question 4.16

If the traces of all powers of a matrix A are 0, what can you say about A?

9.4.17 Question 4.17

When and how can we solve the matrix equation $\exp(A) = B$? Do it over the complex numbers and over the real numbers. give a counterexample with real entries.

9.4.18 Question 4.18

Say we can find a matrix A such that $\exp(A) = B$ for B in $SL_n(\mathbb{R})$. Does A also have to be in $\mathrm{SL}_n(R)$? Does A *need* to be in $SL_n(R)$?

9.4.19 Question 4.19

Is a square matrix always similar to its transpose?

9.4.20 Question 4.20

What are the conjugacy classes of $\mathrm{SL}_2(\mathbb{R})$?

9.4.21 Question 4.21

What are the conjugacy classes in $\mathrm{GL}_2(\mathbb{C})$?

9.5 Matrices and Linear Algebra

9.5.1 Question 5.1

What is a bilinear form on a vector space? When are two forms equivalent? What is an orthogonal matrix? What's special about them?

9.5.2 Question 5.2

What are the possible images of the unit circle under a linear transformation of $\mathbb{R}^2$?

9.5.3 Question 5.3

Explain geometrically how you diagonalise a quadratic form.

9.5.4 Question 5.4

Do you know Witt's theorem on real quadratic forms?

9.5.5 Question 5.5

Classify real division algebras.

9.5.6 Question 5.6

Consider the simple operator on C given by multiplication by a complex number. It decomposes into a stretch and a rotation. What is the generalisation of this to operators on a Hilbert space?

9.5.7 Question 5.7

Do you know about singular value decomposition?

9.5.8 Question 5.8

What are the eigenvalues of a symmetric matrix?

9.5.9 Question 5.9

What can you say about the eigenvalues of a skew-symmetric matrix?

9.5.10 Question 5.10

Prove that the eigenvalues of a Hermitian matrix are real and those of a unitary matrix are unitary.

9.5.11 Question 5.11

Prove that symmetric matrices have real eigenvalues and can be diagonalised by orthogonal matrices.

9.5.12 Question 5.12

To which operators does the spectral theorem for symmetric matrices generalise?

9.5.13 Question 5.13

Given a skew-symmetric/skew-Hermitian matrix S, show that $U = (S + I)(S - I) - 1$ is orthogonal/unitary. Then find an expression for S in terms of U.

9.5.14 Question 5.14

If a linear transformation preserves a nondegenerate alternating form and has k as an eigenvalue, prove that $1/k$ is also an eigenvalue.

9.5.15 Question 5.15

State/prove the Cayley–Hamilton theorem.

9.5.16 Question 5.16

Are diagonalisable $N \times N$ matrices over the complex numbers dense in the space of all $N \times N$ matrices over the complex numbers? How about over another algebraically closed field if we use the Zariski topology?

9.5.17 Question 5.17

For a linear ODE with constant coefficients, how would you solve it using linear algebra?

9.5.18 Question 5.18

What can you say about the eigenspaces of two matrices that commute with each other?

9.5.19 Question 5.19

What is a Toeplitz operator?

9.5.20 Question 5.20

What is the number of invertible matrices over $\mathbb{Z}/p\mathbb{Z}$?

9.6 Rings

9.6.1 Question 6.1

State the Chinese remainder theorem in any form you like. Prove it.

9.6.2 Question 6.2

What is a PID? What's an example of a UFD that is not a PID? Why? Is $k[x]$ a PID? Why?

9.6.3 Question 6.3

Is $\mathbb{C}[x, y]$ a PID? What are the prime ideals in it?

Missing

9.6.4 Question 6.4

Do polynomials in several variables form a PID?

9.6.5 Question 6.5

Prove that the integers form a PID.

9.6.6 Question 6.6

Give an example of a PID with a unique prime ideal.

9.6.7 Question 6.7

What is the relation between Euclidean domains and PIDs?

9.6.8 Question 6.8

Do you know a PID that's not Euclidean?

9.6.9 Question 6.9

Give an example of a UFD which is not a Euclidean domain.

9.6.10 Question 6.10

Is a ring of formal power series a UFD?

9.6.11 Question 6.11

Is a polynomial ring over a UFD again a UFD?

Check?

9.6.12 Question 6.12

What does factorisation over $\mathbb{Q}[x]$ say about factorisation over $\mathbb{Z}[x]$?

9.6.13 Question 6.13

Give an example of a ring where unique factorisation fails.

9.6.14 Question 6.14

Factor 6 in two different ways in $\mathbb{Z}[\sqrt{-5}]$ Is there any way to explain the two factorisations? Factor the ideal generated by 6 into prime ideals.

9.6.15 Question 6.15

What's the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$?

9.6.16 Question 6.16

Find all primes in the ring of Gaussian integers.

9.6.17 Question 6.17

What is a ring of integers? What does "integral over $\mathbb{Z}$" mean?

9.6.18 Question 6.18

Let $\mathcal{O}$ be the ring of integers of $\mathbb{Q}(d)$, where $d > 0$. What can you say about the quotient of O by one of its prime ideals?

9.6.19 Question 6.19

Do you know about Dedekind domains and class numbers?

9.6.20 Question 6.20

Talk about factorisation and primes in a polynomial ring. What is irreducibility? For what rings R is it true that $R[x_1, \cdots, x_n]$ is a unique factorisation domain? What is wrong with unique factorisation if we don't have a domain? Now, PIDs are Noetherian, but are there UFDs which are not?

9.6.21 Question 6.21

What is the radical of an ideal? What is special about elements in the nilradical?

9.6.22 Question 6.22

Define the "radical" of an ideal. Prove it is an ideal. Prove that the ideal of all polynomials vanishing on the zero set of I is $\sqrt{I}$.

9.6.23 Question 6.23.

Do you know what the radical is? Use the fact that the intersection of all prime ideals is the set of all nilpotent elements to prove that $F[x]$ has an infinite number of prime ideals, where F is a field.

9.6.24 Question 6.24

What are the radical ideals in $\mathbb{Z}$?

9.6.25 Question 6.25

Give a prime ideal in $\urcorner[x, y]$. Why is it prime? What is the variety it defines? What is the Nullstellensatz? Can you make some maximal ideals?

9.6.26 Question 6.26

State/describe Hilbert's Nullstellensatz. Sketch a proof.

9.6.27 Question 6.27

What is an irreducible variety? Give an example of a non-irreducible one.

9.6.28 Question 6.28

What are the prime ideals and maximal ideals of $\mathbb{Z}[x]$?

9.6.29 Question 6.29

Missing

9.6.30 Question 6.30

Describe the left, right, and two-sided ideals in the ring of square matrices of a fixed size. Now identify the matrix algebra $\mathrm{Mat}(n \times n, K)$ with $\mathrm{End}_K(V)$ where V is an n-dimensional K-vector space. Try to geometrically describe the simple left ideals and also the simple right ideals via that identification.

9.6.31 Question 6.31

Give examples of maximal ideals in $K = R \times R \times R \times \cdots$, the product of countably many copies of R. What about for a product of countably many copies of an arbitrary commutative ring R?

9.6.32 Question 6.32

Consider a commutative ring, R, and a maximal ideal I, what can you say about the structure of R/I? What if I were prime?

9.6.33 Question 6.33

Define "Noetherian ring". give an example.

9.6.34 Question 6.34

Prove the Hilbert basis theorem.

9.6.35 Question 6.35

What is a Noetherian ring? If I is an ideal in a Noetherian ring with a unit, what is the intersection of I^n over all positive integers n?

9.6.36 Question 6.36

What is the Jacobson radical? If R is a finitely-generated algebra over a field what can you say about it?

9.6.37 Question 6.37

Give an example of an Artinian ring.

9.6.38 Question 6.38

State the structure theorem for semisimple Artinian rings.

9.6.39 Question 6.39

What is a semisimple algebra? State the structure theorem for semisimple algebras.

9.6.40 Question 6.40

What is a matrix algebra?

9.6.41 Question 6.41

Does L_1 have a natural multiplication with which it becomes an algebra?

9.6.42 Question 6.42.

Consider a translation-invariant subspace of L_1. What can you say about its relation to L_2 as a convolution algebra?

9.6.43 Question 6.43

State the structure theorem for simple rings.

9.6.44 Question 6.44

Do you know an example of a local ring? Another one? What about completions?

9.6.45 Question 6.45

Consider the space of functions from the natural numbers to $\mathbb{C}$ endowed with the usual law of addition and the following analogue of the convolution product:

Missing

Show that this is a ring. What does this ring remind you of and what can you say about it?

9.6.46 Question 6.46

Prove that any finite division ring is a field (that is, prove commutativity). Give an example of a (necessarily infinite) division ring which is NOT a field.

9.6.47 Question 6.47

Prove that all finite integral domains are fields.

9.6.48 Question 6.48

Can a polynomial over a division ring have more roots than its degree?

9.6.49 Question 6.49

Classify (finite-dimensional) division algebras over $\mathbb{R}$.

9.6.50 Question 6.50

Give an example of a $\mathbb{C}$-algebra which is not semisimple.

9.6.51 Question 6.51

What is Wedderburn's theorem? What does the group ring generated by $\mathbb{Z}/5\mathbb{Z}$ over $\mathbb{Q}$ look like?

What if we take the noncyclic group of order 4 instead of $\mathbb{Z}/5\mathbb{Z}$? The quaternion group instead of $\mathbb{Z}/5\mathbb{Z}$?

9.6.52 Question 6.52

Tell me about group rings. What do you know about them?

9.7 Modules

9.7.1 Question 7.1

How does one prove the structure theorem for modules over PID? What is the module and what is the PID in the case of abelian groups?

9.7.2 Question 7.2

If M is free abelian, how can I put quotients of M in some standard form? What was crucial about the integers here (abelian groups being modules over $\mathbb{Z}$)? How does the procedure simplify if the ring is a Euclidean domain, not just a PID?

9.7.3 Question 7.3

Suppose D is an integral domain and the fundamental theorem holds for finitely-generated modules over D (i.e. they are all direct sums of finitely many cyclic modules).

Does D have to be a PID?

9.7.4 Question 7.4

Classify finitely-generated modules over $\mathbb{Z}$, over PIDs, and over Dedekind rings.

9.7.5 Question 7.5

Prove a finitely-generated torsion-free abelian group is free abelian.

9.7.6 Question 7.6.

What is a tensor product? What is the universal property? What do the tensors look like in the case of vector spaces?

9.7.7 Question 7.7

Now we'll take the tensor product of two abelian groups, that is, $\mathbb{Z}$-modules. Take $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$, where p and q are distinct primes. What is their tensor product?

9.7.8 Question 7.8

What is a projective module?

9.7.9 Question 7.9

What is an injective module?

9.7.10 Question 7.10

Do you know an example of a flat module?

9.8 Representation Theory

9.8.1 Question 8.1

Define “representation” of a group. Define “irreducible representation”. Why can you decompose representations of finite groups into irreducible ones? Construct an in- variant inner product.

9.8.2 Question 8.2

State and prove Maschke’s theorem. What can go wrong if you work over the real field? What can go wrong in characteristic p?

9.8.3 Question 8.3

Do you know what a group representation is? Do you know what the trace of a group representation is?

9.8.4 Question 8.4

State/prove/explain Schur’s lemma.

9.8.5 Question 8.5

What can you say about characters? What are the orthogonality relations? How do you use characters to determine if a given irreducible representation is a subspace of another given representation?

9.8.6 Question 8.6

What’s the relation between the number of conjugacy classes in a finite group and the number of irreducible representations?

9.8.7 Question 8.7

What is the character table? What field do its entries lie in?

9.8.8 Question 8.8

Why is the character table a square?

9.8.9 Question 8.9

If $\chi(g)$ is real for every character χ, what can you say about g?

9.8.10 Question 8.10

What's the regular representation?

9.8.11 Question 8.11

Give two definitions of "induced representation". Why are they equivalent?

9.8.12 Question 8.12

If you have a representation of H, a subgroup of a group G, how can you induce a representation of G?

9.8.13 Question 8.13

If you have an irreducible representation of a subgroup, is the induced representation of the whole group still irreducible?

9.8.14 Question 8.14.

What can you say about the kernel of an irreducible representation? How about kernels of direct sums of irreducibles? What kind of functor is induction? Left or right exact?

9.8.15 Question 8.15

What is Frobenius reciprocity?

9.8.16 Question 8.16

Given a normal subgroup H of a finite group G, we lift all the representations of G/H to representations of G.

Show that the intersection of the kernels of all these representations is precisely H. What can you say when H is the commutator subgroup of G?

9.8.17 Question 8.17

If you have two linear representations π_1 and π_2 of a finite group G such that $\pi_1(g)$ is conjugate to $\pi_2(g)$ for every g in G, is it true that the two representations are isomorphic?

9.8.18 Question 8.18

Group representations: What's special about using $\mathbb{C}$ in the definition of group algebra?

Is it possible to work over other fields?

What goes wrong if the characteristic of the field divides the order of the group?

9.8.19 Question 8.19

Suppose you have a finite p-group, and you have a representation of this group on a finite-dimensional vector space over a finite field of characteristic p. What can you say about it?

9.8.20 Question 8.20

Let (π, V) be a faithful finite-dimensional representation of G. Show that, given any irreducible representation of G, the nth tensor power of $\mathrm{GL}(V)$ will contain it for some large enough n.

9.8.21 Question 8.21

What are the irreducible representations of finite abelian groups?

9.8.22 Question 8.22

What are the group characters of the multiplicative group of a finite field?

9.8.23 Question 8.23

Are there two nonisomorphic groups with the same representations?

9.8.24 Question 8.24

If you have a $\mathbb{Z}/5\mathbb{Z}$ action on a complex vector space, what does this action look like? What about an S_3 action? A dihedral group of any order?

9.8.25 Question 8.25

What are the representations of S_3? How do they restrict to S_2?

9.8.26 Question 8.26

Tell me about the representations of D_4. Write down the character table. What is the 2-dimensional representation? How can it be interpreted geometrically?

9.8.27 Question 8.27

How would you work out the orders of the irreducible representations of the dihedral group D_n?

Why is the sum of squares of dimensions equal to the order of the group?

9.8.28 Question 8.28

Do you know any representation theory? What about representations of A_4?

Give a nontrivial one. What else is there? How many irreducible representations do we have? What are their degrees? Write the character table of A_4.

9.8.29 Question 8.29

Write the character table for S_4.

9.8.30 Question 8.30

Start constructing the character table for S_5.

9.8.31 Question 8.31.

How many irreducible representations does S_n have?

What classical function in mathematics does this number relate to?

9.8.32 Question 8.32

Discuss representations of $\mathbb{Z}$, the infinite cyclic group. What is the group algebra of $\mathbb{Z}$?

What is the connection

Incomplete question

9.8.33 Question 8.33

What is a Lie group? Define a unitary representation. What is the Peter– Weyl theorem? What is the Lie algebra? The Jacobi identity? What is the adjoint representation of a Lie algebra? What is the commutator of two vector fields on a manifold?

When is a representation of $\mathbb{Z}$ completely reducible? Why?

Which are the indecomposable modules?

9.8.34 Question 8.34

Talk about the representation theory of compact Lie groups. How do you know you have a finite-dimensional representation?

9.8.35 Question 8.35

How do you prove that any finite-dimensional representation of a compact Lie group is equivalent to a unitary one?

9.8.36 Question 8.36

Do you know a Lie group that has no faithful finite-dimensional representations?

9.8.37 Question 8.37

What do you know about representations of SO(2)? SO(3)?

9.9 Categories and Functors

9.9.1 Question 9.1

Which is the connection between Hom and tensor product? What is this called in representation theory?

9.9.2 Question 9.2

Can you get a long exact sequence from a short exact sequence of abelian groups together with another abelian group?

9.9.3 Question 9.3

Do you know what the Ext functor of an abelian group is? Do you know where it appears? What is $\mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$? What is $\mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})$?

10 Appendix: Extra Topics

10.1 Characteristic Subgroups

Definition 10.1.1 (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 10.1.2 (Normal Core of a subgroup)
The largest normal subgroup of G containing H:

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

where

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

Definition 10.1.3 (Characteristic subgroup)
$H \leq G$ is *characteristic* iff H is fixed by every element of $\mathrm{Aut}(G)$.

Theorem 10.1.4 ***(Fratini's Argument).***
If $H \trianglelefteq G$ and $P \in \mathrm{Syl}_p(G)$, then $HN_G(P) = G$ and $[G : H]$ divides $|N_G(P)|$.

10.2 Nilpotent Groups

Definition 10.2.1 (Nilpotent)
A group G is **nilpotent** iff G has a terminating upper central series.

Moral: the adjoint map is nilpotent.

Theorem 10.2.2 ***(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 10.2.3 ***(Nilpotent Implies Maximal Normals).***
A group G is nilpotent iff every maximal subgroup is normal.

Theorem 10.2.4 ***(Characterization of Nilpotent Groups).***
G is nilpotent iff G has an upper central series terminating at G.

Theorem 10.2.5 ***(Characterization of Nilpotent Groups).***
G is nilpotent iff G has a lower central series terminating at 1.

Proposition 10.2.6.
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.
- G has normal subgroups of order d for *every* d dividing $|G|$

Todo. Speci

Bibliography

[1] David Steven. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley and Sons, 2004.

[2] Kenneth Hoffman and Ray Kunze. *Linear Algebra*. Prentice Hall, 1981.

[3] Thomas W. Hungerford. *Algebra*. Springer, 2008.

[4] Roy Smith. *Algebra Notes by Roy Smith*. URL: `https://www.math.uga.edu/directory/people/roy-smith`.