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 Dummit and Foote are excellent. All the definitions and proofs of these theorems on groups are given in Smith's web based lecture notes for math 843 part 1."

1.2.1 Topics

Chapters 1-9 of Dummit and Foote

- **The first isomorphism theorem**,
- Fundamental theorem of finite abelian groups
- Left and right cosets
- Normalizer

- Lagrange's theorem
- Isomorphism theorems
- Lagrange's Theorem
- Group generated by a subset
- Subgroups and quotient groups
- Fundamental homomorphism theorems
- Direct and semi-direct products
  - Recognition of internal direct product
  - Recognition of semi-direct product
- Composite groups
- Structures of special types of groups such as:
  - p-groups
  - Dihedral,
    - ♢ Cyclic groups
    - ♢ Free groups
      - ♢ Generators and relations
  - Symmetric and Alternating groups
    - ♢ Cycle decompositions
- Group actions with applications to the structure of groups such as
  - **The Sylow Theorems**
    - ♢ Proof of Sylow theorems
  - Orbit stabilizer theorem
  - Orbits act on left cosets of subgroups
  - Action of G on itself by conjugation
  - Class equation
  - Cayley's theorem
- The simple groups of order between 60 and 168 have prime order
- The simplicity of A_n, for $n \geq 5$
- Solvable groups
- Subgroups of index p, the smallest prime dividing $\#G$, are normal

- p-groups
- p^2 groups are abelian
- Automorphisms
  - Inner automorphisms
- A_n is simple for $n \geq 5$
- Classification of groups of order pq
- Commutator subgroup
- Nilpotent groups
- Upper central series
- Lower central series
- Derived series
- Solvable groups
- Fratini's argument
- The Jordan Holder theorem

*The proof of Jordan-Holder is seldom tested on the qual**, but proofs are always of interest.*

1.3 Linear Algebra

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

1.3.1 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]

- 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)
- DF Chapters 7, 8, 9.

1.4.1 Topics

- Properties of ideals and quotient rings
- The fundamental isomorphism theorems for rings
- I maximal iff R/I is a field
- Zorn's lemma
  - Every vector space has a basis
  - Maximal ideals exist
  - Construct algebraic field closures
  - Why it is unnecessary in countable or noetherian rings.

Smith discusses extensively in 844-1.

- Chinese Remainder Theorem
- Euclidean algorithm
- Primes and irreducibles

- Gaussian integers
- Localization of a domain
- Field of fractions
- Factorization in domains
- Factorization in $Z[i]$
- 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
    - ♢ 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)*
  - Euclidean domains
    - ♢ Are PIDs
- 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
- Polynomial rings
- Polynomials
  - Gauss' lemma
  - Remainder and factor theorem
  - Eisenstein's criterion *(DF p.309)* > Stated only for monic polynomials – proof of general case identical. > See Smith's notes for the full version.

  - Reducibility
  - Rational root test

- 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 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 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
  - of cyclotomic polynomials
- Solvability of polynomials by radicals

2 Group Theory

2.1 Big List of Notation

Remark 2.1.1 ***(Notation):*** I use the following notation throughout:

Notation	Definition
$C_G(x)$	Centralizer of an element $:= \left\{ g \in \Gamma \;\middle|\; [g,x] = 1 \right\} \subseteq \Gamma$
$C_G(H)$	Centralizer of an subgroup $:= \left\{ g \in \Gamma \;\middle|\; [g,x] = 1 \ \forall h \in H \right\} = \bigcap_{h \in H} C_H(h) \subseteq G$
$C(H)$	Conjugacy Class $:= \left\{ ghg^{-1} \;\middle|\; g \in G \right\} \leq G \subseteq G$
$Z(G)$	Center $:= \left\{ x \in G \;\middle|\; \forall g \in G,\, gxg^{-1} = x \right\} \subseteq G$
$N_G(H)$	Normalizer $:= \left\{ g \in G \;\middle|\; gHg^{-1} = H \right\} \subseteq G$
$\mathrm{Inn}(G)$	Inner Automorphisms $:= \left\{ \varphi_g(x) := gxg^{-1} \right\} \subseteq \mathrm{Aut}(G)$
$\mathrm{Out}(G)$	Outer Automorphisms $\mathrm{Aut}(G)/\mathrm{Inn}(G) \mapsfrom \mathrm{Aut}(G)$
$[gh]$	Commutator of Elements $:= ghg^{-1} \in G$
$[GH]$	Commutator of Subgroups $:= \left\langle \left\{ [gh] \;\middle|\; g \in G,\, h \in H \right\} \right\rangle \leq G$

Notation	Definition
$\mathcal{O}_x$, Gx	Orbit of an Element $:= \left\{ gx \mid x \in X \right\}$
$\mathrm{Stab}_G(x)$, G_x	Stabilizer of an Element $:= \left\{ g \in G \mid gx = x \right\} \subseteq G$
X/G	Set of Orbits $:= \left\{ G_x \mid x \in X \right\} \subseteq 2^X$
X^g	Fixed Points $\left\{ x \in X \mid \forall g \in G,\ gx = x \right\} \subseteq X$
2^X	The powerset of X $:= \{U \subseteq X\}$

Remark 2.1.2: For any p dividing the order of G, $\mathrm{Syl}_p(G)$ denotes the *set* of Sylow-p subgroups of G.

2.2 Definitions

Fact 2.2.1
An set morphism that is *either* injective or surjective between sets of the same size is automatically a bijection. Consequently, a group morphism between groups of the same size that is either injective or surjective is automatically an isomorphism.

Fact 2.2.2 (The division algorithm)
If $a, b \in \mathbb{Z}$ with $\gcd(a, b) = d$, then there exist $s, t \in \mathbb{Z}$ such that

$$as + bt = d.$$

Remark 2.2.3: Useful context clue! In particular, this works when a, b are coprime and $d = 1$. If you see “coprime” in a finite group question, try the division algorithm.

Definition 2.2.4 (Order)
The **order** of an element $g \in G$, denoted $n := o(g)$, is the smallest $n \in \mathbb{Z}^{\geq 0}$ such that $g^n = e$.

Exercise 2.2.5 (?)
Show that the order of any element in a group divides the order of the group.

Definition 2.2.6 (Commutator)
The **commutator subgroup** of G is denoted $[G, G] \leq G$. It is the subgroup generated by all

elementary commutators:

$$[G,G] := \left\langle aba^{-1}b^{-1} \;\middle|\; a,b\in G\right\rangle .$$

It is the smallest normal subgroup $N \trianglelefteq G$ such that G/N is abelian, so if $H \leq G$ and G/H is abelian, $H \subseteq [G,G]$.

Definition 2.2.7 (Group Presentation)
An expression of the form $G = \left\langle S \;\middle|\; R\right\rangle$ where S is a set of elements and R a set of words defining relations means that $G := F[S]/\mathrm{cl}_n(R)$ where $F[S]$ is the free group on the set S and $\mathrm{cl}_n(R)$ is the normal closure, the smallest normal subgroup of $F[S]$ containing R.

Remark 2.2.8: Finding morphisms between presentations: if G is presented with generators g_i with relations r_i and H is any group containing elements h_i also satisfying r_i, there is a group morphism

$$\begin{aligned} \varphi : G &\to H \\ g_i &\mapsto h_i \quad \forall i. \end{aligned}$$

Why this exists: the presentation yields a morphism $\pi : F(g_i) \to G$ with $G \cong F(g_i)/\ker\pi$. Define a map $\psi : F(g_i) \to H$ where $g_i \mapsto h_i$, then since the h_i satisfy the relations r_i, $\ker\pi \subseteq \ker\psi$. So ψ factors through $\ker\pi$ yielding a morphism $F/\ker\pi \to H$.

2.3 Subgroups

Definition 2.3.1 (Subgroup)
A subset $H \subseteq G$ is a **subgroup** iff

1. Closure: $HH \subset H$
2. Identity: $e \in H$
3. Inverses: $g \in H \iff g^{-1} \in H$.

Exercise 2.3.2 (Unions of subgroups)
Show that if $K, H \leq G$ are subgroups, then their union $H \cup K$ is a subgroup iff (wlog) $H \subset K$.

Definition 2.3.3 (Subgroup Generated by a Subset)
If $H \subset G$, then $\langle H\rangle$ is the smallest subgroup containing H:

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

where adjacent h_i are distinct.

Proposition 2.3.4 ***(One-step subgroup test).***
If $H \subseteq G$ and $a, b \in H \implies ab^{-1} \in H$, then $H \leq G$.

Proof (of the one-step subgroup test).

- Identity: $a = b = x \implies xx^{-1} = e \in H$
- Inverses: $a = e, b = x \implies x^{-1} \in H$.
- Closure: let $x, y \in H$, then $y^{-1} \in H$ by above, so $xy = x(y^{-1})^{-1} \in H$.

■

Exercise 2.3.5 (Coprime order implies disjoint)
Show that coprime order subgroups are disjoint, or more generally $\mathbb{Z}_p, \mathbb{Z}_q \subset G \implies \mathbb{Z}_p \cap \mathbb{Z}_q = \mathbb{Z}_{(p,q)}$.

Proposition 2.3.6 ***(Intersection of subgroups is a subgroup).***
If $H, K \leq G$ then $J := H \cap K \leq G$ is a subgroup. Moreover $J \leq H$ and $J \leq K$.

Proof (?).
One-step subgroup test.

■

Exercise 2.3.7 (?)

- 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.

2.4 Conjugacy

Definition 2.4.1 (Conjugacy class)
The **conjugacy class** of h is defined as

$$C(h) := \left\{ ghg^{-1} \;\middle|\; g \in G \right\}.$$

Remark 2.4.2: $[e] = \{e\}$ is always in a conjugacy class of size one – this is useful for counting and divisibility arguments. Conjugacy classes are **not** subgroups in general, since they don't generally contain e. However, by orbit-stabilizer and the conjugation action, their sizes always divide the order of G.

Also note that$[x] = \{x\} \iff x \in Z(G)$, i.e. having a trivial conjugacy class is the same as being central.

Definition 2.4.3 (Conjugate subgroups)
Two subgroups $H, K \leq G$ are **conjugate** iff there exists some $g \in G$ such that $gHg^{-1} = K$. Note that all conjugates have the same cardinality.

Exercise 2.4.4 (?)
Show that the size of a conjugacy class divides the order of a group.

Exercise 2.4.5 (?)
Show that if $H < G$ is a proper subgroup, then $\bigcup_{g \in G} gHg^{-1} \subset G$ is a proper subset.

Hint: consider the intersection and count. Try Orbit-stabilizer?

Solution:
Strategy: bound the cardinality. All conjugates of H have the same cardinality, say $\#H = m$. Suppose there are n distinct conjugates of H. Then they intersect only at the identity, so count their elements:

$$\# \bigcup_{g \in G} gHg^{-1} = 1 + n(m-1).$$

Use that $n = [G : N_G(H)]$ by Orbit-Stabilizer, and $N_G(H) \leq G \implies n \leq n' \coloneqq [G : H]$. Now note $n'm = \#H[G : H] = \#G$ by Lagrange:

$$\begin{aligned}
\# \bigcup_{g \in G} gHg^{-1} &= 1 + n(m-1) \\
&\leq 1 + n'(m-1) \\
&= 1 + n'm - n' \\
&= 1 + \#G - n' \\
&= \#G - (n' - 1) \\
&< \#G && \iff n' \coloneqq [G : H] > 1.
\end{aligned}$$

Exercise 2.4.6 (?)
Show that normal groups absorb conjugacy classes: if $N \trianglelefteq G$ and $[g_i]$ is a conjugacy class in g, either $[g_i] \subseteq N$ or $[g_i] \cap N = \emptyset$.

Exercise 2.4.7 (?)
Prove that the size of a conjugacy class of g_i is the index of its centralizer, $[G : Z(g_i)] \coloneqq [G : C_G(g_i)]$.

2.4.1 Normal Subgroups

Definition 2.4.8 (Normal subgroup)
A subgroup $N \leq G$ is **normal** iff $gH = Hg$ for every $g \in G$, or equivalently $gHg^{-1} = H$ for all g, so H has only itself as a conjugate. We denote this by $N \trianglelefteq G$. Equivalently, for every inner automorphism $\psi \in \operatorname{Inn}(G)$, $\psi(N) = N$.

Proposition 2.4.9 ***(Normal iff disjoint union of conjugacy classes).***
$N \trianglelefteq G \iff N = \coprod' [h_i]$ is a disjoint union of conjugacy classes, where the index set for this union is one h_i from each conjugacy class.

Proof (?).
Note that $C(h_i) = \left\{ gh_ig^{-1} \;\middle|\; g \in G \right\}$, and $gh_ig^{-1} \in H$ since H is normal, so $C(h_i) \subseteq G$ for all i. Conversely, if $C(h_i) \subseteq H$ for all $h_i \in H$, then $gh_ig^{-1} \in H$ for all i and H is normal. ■

Exercise 2.4.10 (?)
- Show that if $H, K \trianglelefteq G$ and $H \cap K = \emptyset$, then $hk = kh$ for all $h \in H, k \in K$.
- Show that if $H, K \trianglelefteq G$ are normal subgroups that intersect trivially, then $[H, K] = 1$ (so $hk = kh$ for all k and h).

Exercise 2.4.11 (?)
Prove that if G is a p-group, every subgroup $N \trianglelefteq G$ intersects the center $Z(G)$.

2.5 Centralizing and Centers

Definition 2.5.1 (Centralizer)
The centralizer of an en element is defined as

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

the elements of G the stabilize h under conjugation.
The **centralizer of a subset** H is defined as

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

the elements of G that simultaneously stabilize all of H pointwise under conjugation.

Definition 2.5.2 (Normalizer)

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

Contrast to the centralizer: these don't have to fix H pointwise, but instead can permute elements of H.

Remark 2.5.3: $C_G(S) \trianglelefteq N_G(H)$ for any H.

Proposition 2.5.4 ***(NC Theorem).***
$N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Definition 2.5.5 (Normalizers Grow)
If for every proper $H < G$, $H \trianglelefteq N_G(H)$ is again proper, then "normalizers grow" in G.

Definition 2.5.6 (Center)

$$Z(G) = \left\{ g \in G \;\middle|\; [g,h] = e \,\forall h \in H \right\} = \left\{ g \in G \;\middle|\; Z(g) = G \right\},$$

the subgroup of *central* elements: those $g \in G$ that commute with every element of G.

Exercise 2.5.7 (?)

- 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 $Z(G)$.

2.6 Cosets

Proposition 2.6.1 ***(Tower law for subgroups).***

$$K \leq H \leq G \implies [G:K] = [G:H][H:K].$$

Proposition 2.6.2 ***(Indices grow).***
If $H, K \leq G$, then

$$[H : H \cap K] \leq [G : K].$$

Proof (?).
Write $G/H \cap K \coloneqq G/J = \{h_1 J, \cdots, h_m J\}$ as distinct cosets. Then $i \neq j \implies h_i h_j^{-1} \notin H \cap K$, but $h_i h_j^{-1} \in H$ since $H \leq G$, which forces $h_i h_j^{-1} \notin K$. So $h_i K \neq h_j K$, meaning there are at least m cosets in G/K.

■

Proposition 2.6.3 ***(Cosets are identical or disjoint).***
Any two cosets xH, yH are either identical or disjoint.

Proof (?).
Note $x \in xH$, since $e \in H$ because H is a subgroup and we can take $h = e$ to get $x = xe := xh \in xH$. The reverse containment is clear, so $G = \cup_{x \in G} xH$ is a union of its cosets. Suppose toward a contradiction that $\ell \in xH \cap yH$ we'll show $xH = yH$. Write $\ell = xh_1 = yh_2$ for some h_i, then

$$\begin{aligned} xh_1 = yh_2 &\implies x = yh_2h_1^{-1} \\ xh_3 \in xH &\implies xh_3 = (yh_2h_1^{-1})h_3 \in yH, \end{aligned}$$

so $xH \subseteq yH$. A symmetric argument shows $y_H \subseteq xH$. [a]

■

[a] See full argument: D&F p.80.

Theorem 2.6.4 ***(The Fundamental Theorem of Cosets).***

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

Proof (?).
[a]

$$aH = bH \iff a \in bH \iff a = bh \text{ for some } h \iff b^{-1}a = h \iff ba^{-1} \in H.$$

■

[a] See full argument: D&F p.80.

Definition 2.6.5 (Index of a subgroup)
The **index** $[G : H]$ of a subgroup $H \leq G$ is the number of left (or right) cosets gH.

Remark 2.6.6 ***(Common coset trick):*** If you can reduce a problem to showing $X \subseteq H$, it suffices to show $xH = H$ for all $x \in X$.

Remark 2.6.7: Cosets form an equivalence relation and thus partition a group. Nice trick: write $G/H = \{g_1H, g_2H, \cdots, g_nH\}$, then $G = \coprod_{i \leq n} g_iH$.

Theorem 2.6.8 ***(Counting Cosets).***
If $H \trianglelefteq G$ and G is finite then

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

Exercise 2.6.9 (?)
Show that if G is finite then $|G|/|H| = [G : H]$.

2.7 Special Groups

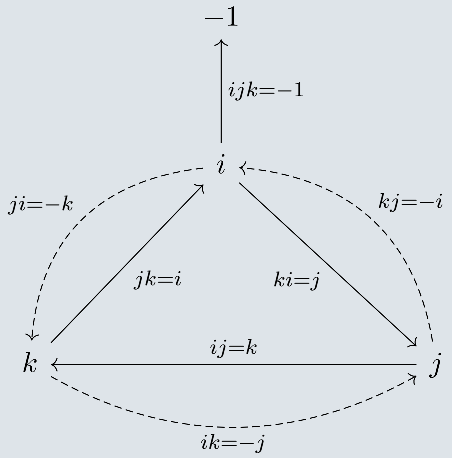
Definition 2.7.1 (The Dihedral Group)
A **dihedral group** of order $2n$ is given by

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

Definition 2.7.2 (The Quaternion Group)
The **Quaternion group** of order 8 is given by

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

Mnemonic: multiply clockwise to preserve sign, counter-clockwise to negate sign. Everything squares to -1, and the triple product is -1:



Link to Diagram

Definition 2.7.3 (Transitive Subgroup)
A subgroup of S_n is **transitive** iff its action on $\{1, 2, \cdots, n\}$ is transitive.

Definition 2.7.4 (p-groups)
If $|G| = p^k$, then G is a **p-group.**

2.7.1 Cyclic Groups

Theorem 2.7.5 ***(Subgroups of Cyclic Groups).***
G is cyclic of order $n := \#G$ iff G has a unique subgroup of order d for each d dividing n.

Proof (?).
$\Longleftarrow$: Use that $\sum_{d \mid n} \varphi(d) = n$, and that there are at most $\varphi(d)$ elements of order d, forcing equality.
$\Longrightarrow$: If $G = \langle a \rangle$ with $a^n = e$, then for each $d \mid n$ take $H_d := \left\langle a^{\frac{n}{d}} \right\rangle$ for existence. ■

Exercise 2.7.6 (?)

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

2.7.2 Symmetric Groups

Definition 2.7.7 (The symmetric group)
The transposition presentation:

$$S_n := \left\langle \sigma_1, \cdots, \sigma_{n-1} \;\middle|\; \sigma_i^2, [\sigma_i, \sigma_j]\,(j \neq i+1), \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \right\rangle.$$

Definition 2.7.8 (The sign homomorphism)
Defined by the map

$$\begin{aligned} \mathrm{sgn} : S_n &\to (\mathbb{Z}/2, +) \\ \prod_{i \leq 2k} (a_i b_i) &\mapsto 0 \\ \prod_{i \leq 2k+1} (a_i b_i) &\mapsto 1. \end{aligned}$$

- The kernel is the alternating group, cycles that
  - **Even** cycles
  - For a single cycle: has **odd** length

  - Have an **even** number of even length cycles.
  - Can be written as an **even** number of transpositions

- The fiber over 1 is everything else:
  - **Odd** cycles
  - For a single cycle: has **even** length
  - Have an **odd** number of even length cycles.
  - Can be written as an **odd** number of transpositions

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

Definition 2.7.9 (Alternating Group)
The **alternating group** is the subgroup of **even** permutations, i.e.

$$A_n := \left\{ \sigma \in S_n \;\middle|\; \operatorname{sgn}(\sigma) = 0 \right\}$$

Proposition 2.7.10 ***(A_n is generated by 3-cycles).***
For $n \geq 3$, A_n is generated by 3-cycles.

Proof (?).
Every 3-cycle (abc) is even, and thus in A_n. Given an arbitrary even permutation $(t_1 \ldots t_{2k})$, it decomposes into a product of an odd number of transpositions $(t_{2j-1}t_{2j})$. So it suffices to write every such transposition as a 3-cycle. There are only 3 cases the occur:

- $(ab)(ab) = ()$
- $(ab)(ac) = (abc)$
- $(ab)(cd) = (abc)(adc)$.

■

Example 2.7.11 ***(Of an explicit alternating group):***

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

Fact 2.7.12 (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 disjoint cycles.
- Disjoint cycles commute.
- $A_{n\geq 5}$ is *simple*.

2.8 Exercises

Exercise 2.8.1 (?)

- Show that if G is a finite group acting transitively on a set X with at least two elements, then there exists $g \in G$ which fixes no point of X.
- Let p be prime. For each abelian group K of order p^2, how many subgroups $H \leq \mathbb{Z}^{\times 3}$ are there with $\mathbb{Z}^3/H \cong K$?
- Let $\#G = pq$, with p, q distinct primes. Show that G has a nontrivial proper normal subgroup, and if $p \not\equiv 1 \pmod{q}$ and $q \not\equiv 1 \pmod{p}$ then G is abelian.
- Let G be a finite group and let p be the smallest prime dividing $\#G$, and assume G has a normal subgroup of order p. Show that $H \subset Z(G)$.
- Let G be finite and P a Sylow 2-subgroup. Assume P is cyclic and generated by x. Show that the sign of the permutation of G corresponding to $x \mapsto gx$ is 1, and deduce that G has a nontrivial quotient of order 2.

2.9 Counting Theorems

Theorem 2.9.1 ***(Lagrange's Theorem).***

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

Moreover, there is an equality $[G : H] = \#G/\#H$ when G is finite.

Proof (of Lagrange's theorem).
Write $G/H = \{g_0 H, g_1 H, \cdots, g_N H\}$ for some $N := [G : H]$. Since cosets are equal or disjoint and have equal cardinality,

$$G = \coprod_{k\leq N} g_k H \implies \#G = \sum_{k\leq N} \#(g_k H) = \sum_{k\leq N} \#H = N\#H,$$

so $\#G = N\#H$, $\#H$ divides $\#G$ and $N = [G : H]$ divides $\#G$.

■

Corollary 2.9.2 *(?).*

$$\#G = \#(G/H)\#H \coloneqq [G:H]\,\#H,$$

or written another way,

$$\#(G/H) = \#G/\#H.$$

Corollary 2.9.3.
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 2.9.4
There do **not** necessarily exist $H \leq G$ with $|H| = n$ for every $n \mid |G|$. Counterexample: take $G = A_5$, then $\#G = 5!/2 = 60$ but G has no subgroup of order 30. If it did, this would be index 2 and thus normal, but $A_{n\geq 5}$ is simple.

Another direct counterexample: $|A_4| = 12$ but has no subgroup of order 6. If such an H existed, it can't contain every 3-cycle, since A_4 is generated by 3-cycles. For x any 3-cycle *not* in H, use that $\#A_4/H = 2$ and consider H, xH, x^2H. $x \notin H$, so $H \neq xH$, but two must be equal:

- $x^2H = H$: use $x^2 = x^{-1}$ since $x^3 = e$, but $x \in H \implies x^{-1} \in H$, ↯
- $xH = x^2H$: the fundamental theorem of cosets forces $x^{-1}x^2 \in H$, so $x \in H$. ↯

Theorem 2.9.5 *(Cauchy's Theorem).*
For every prime p dividing $|G|$. there is an element (and thus a subgroup) of order p.

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

Proof (?).
See https://kconrad.math.uconn.edu/blurbs/grouptheory/cauchypf.pdf. ■

2.10 Group Actions

Definition 2.10.1 (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

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

satisfying

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

Fact 2.10.2
For any group action, the kernel is the intersection of all stabilizers:

$$\ker \psi = \bigcap_{x \in X} G_x.$$

Definition 2.10.3 (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.

Proposition 2.10.4 ***(Orbit Stabilizer Isomorphism).***
If $G \curvearrowright X$ transitively, then for any choice of $x \in X$ there is an isomorphism of sets given by

$$\begin{aligned} \Phi : G/G_x &\xrightarrow{\sim} X \\ gG_x &\mapsto g \curvearrowright x. \end{aligned}$$

Proof (?).

- Injectivity: $\Phi(gG_x) = \Phi(hG_x) \iff g \curvearrowright x = h \curvearrowright x \iff gh^{-1} \curvearrowright x = x \iff gh^{-1} \in G_x \iff gG_x = hG_x$.
- Well-definedness: use $gG_x = hG_x \iff gh^{-1} \in G_x \iff g^{-1}h \curvearrowright x = x$. Then $g(g^{-1}h) \curvearrowright x = g \curvearrowright x$ on one hand, and on the other $(gg^{-1})h \curvearrowright x = h \curvearrowright x$, so

$$\Phi(hG_x) \coloneqq h \curvearrowright x = (gg^{-1})h \curvearrowright x = g(g^{-1}h) \curvearrowright x = g \curvearrowright x = \Phi(gG_x).$$

- Surjectivity: equivalent to the action being transitive.

■

Proposition 2.10.5 ***(?).***
If $X \in G$-Set where $G \curvearrowright X$ transitively, then for any points $x_i \in X$, the stabilizers G_{x_0} and G_{x_1} are conjugate.

Prove

Proof (?).

- Injectivity: check that $\varphi(\bar{g}) = \varphi(\bar{h}) \iff g \curvearrowright x_0 = h \curvearrowright x_0 \iff gh^{-1} \in G_{x_0}$.
- Surjectivity: follows from transitivity.

$\blacksquare$

Remark 2.10.6 ***(Reminder of notation):*** For a group G acting on a set X,

Notation	Definition
$\mathcal{O}(x) = Gx = \left\{ g \cdot x \;\middle|\; g \in G \right\} \subseteq X$	Orbit
$\operatorname{Stab}(x) = G_x = \left\{ g \in G \;\middle|\; g \cdot x = x \right\} \leq G$	Stabilizer
$X/G \subseteq 2^X$	Set of Orbits
$\operatorname{Fix} = X^G = \left\{ x \in X \;\middle|\; g \cdot x = x \,\forall g \in G \right\} \subseteq X$	Set of 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. Also, $x \in \operatorname{Fix}$ iff $\operatorname{Orb}(x) = \{x\}$ and $\operatorname{Stab}_G(x) = G$.

Theorem 2.10.7 ***(Orbit-Stabilizer).***

$$\# Gx = [G : G_x] = \# G / \# G_x \quad \text{if } G \text{ is finite.}$$

Mnemonic: $G/G_x \cong Gx$.

2.11 Examples of Orbit-Stabilizer and the Class Equation

Example 2.11.1 ***(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.
  - This action is transitive.
- The set of fixed points $\operatorname{Fix} = \left\{ g \in G \;\middle|\; gx = x \,\forall x \in G \right\} = \{e\}$ is just the identity.
- The stabilizer $G_x = \left\{ g \in G \;\middle|\; gx = x \right\} = \{e\}$ is just the identity.
- The kernel is the identity.

2.11.1 The Class Equation and Burnside's Lemma

Example 2.11.2 ***(Conjugation yields centers/centralizers):*** Let G act on *itself* by conjugation.

- The orbit $\mathcal{O}(g) = C(g)$ is the **conjugacy class** of x.
  - Thus the action is transitive iff there is one conjugacy class.
- The set of fixed points $\operatorname{Fix} = Z(G)$ is the **center**.
- The stabilizer is $\operatorname{Stab}(g) = Z(g) = C_G(g)$, the **centralizer** of g.
- The kernel is the intersection of all centralizers, i.e. again the **center** $Z(G)$.

Remark 2.11.3: 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.

Remark 2.11.4: Directly interpreting this using the orbit-stabilizer formula, the size of a conjugacy class $C(x)$ is the index of its centralizer, $[G : Z(x)]$, i.e.

$$\#C(x) = [G : Z(x)].$$

Now note that $G = \coprod_k' \operatorname{Orb}(h_k)$ is a disjoint union of orbits (the prime denotes taking one representative from each orbit), and so

$$\begin{aligned} G &= \coprod_k{}' \operatorname{Orb}(h_k) \xrightarrow{\sim} \coprod_k{}' G/\operatorname{Stab}(h_k) \\ \implies \#G &= \sum_k{}' \#C(h) = \sum_k{}' \#(G/\operatorname{Stab}(h_k)) = \sum_k{}' [G : Z(h_k)]. \end{aligned}$$

Pulling out the terms of size 1, we have $[G : N_G(h_k)] = 1 \iff h_k \in Z(G)$, which yields the class equation:

Corollary 2.11.5 ***(The Class Equation).***

$$|G| = |Z(G)| + \sum_{\substack{\text{One } g \text{ from} \\ \text{each nontrivial} \\ \text{conj. class}}} [G : Z(g)]$$

Proposition 2.11.6 ***(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 2.11.7 ***(Burnside's Lemma).***
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 of fixed points, i.e.

Proof (of Burnside's Lemma).
Strategy: form the set $A \coloneqq \left\{ (g,x)\in G\times X \;\middle|\; g \curvearrowright x = x \right\}$ and write/count it in two different ways. First union over G:

$$A = \coprod_{g\in G}\left\{ (g,x) \;\middle|\; gx = x\right\} \cong \coprod_{g\in G}\{g\}\times X^g.$$

Then union over X:

$$A = \coprod_{x\in X}\left\{ (g,x) \;\middle|\; gx = x\right\} \cong \coprod_{x\in X} G_x\times \{g\}.$$

Taking cardinalities, and using the fact that $\{p\}\times A \cong A$ as sets for any set A,

$$\coprod_{g\in G} X^g \cong \coprod_{x\in X} G_x \implies \sum_{g\in G}\#X^g = \sum_{x\in X}\#G_x.$$

Apply orbit-stabilizer:

$$\begin{aligned}\#G_x = \frac{\#G}{\#Gx} \implies \sum_{g\in G} X^g &= \sum_{x\in X}\#G_x \\ &= \sum_{x\in X}\frac{\#G}{\#Gx} \\ &= \#G\sum_{x\in X}\frac{1}{\#Gx},\end{aligned}$$

so it suffices to show $\sum_{x\in X}\frac{1}{\#Gx} = \#X/G$. Proceed by grouping terms in this sum according to which orbit they're in:

$$\begin{aligned}\sum_{x\in X}\frac{1}{\#Gx} &= \sum_{Gx\in X/G}\sum_{y\in Gx}\frac{1}{\#Gx} \\ &= \sum_{Gx\in X/G}\frac{1}{\#Gx}\sum_{y\in Gx}1 \\ &= \sum_{Gx\in X/G}\frac{1}{\#Gx}\#G_x \\ &= \sum_{Gx\in X/G}1 \\ &= \#X/G.\end{aligned}$$

■

2.11.2 Conjugation on Subgroups

Example 2.11.8 ***(?):*** Let G act on $X := \left\{ H \;\middle|\; H \leq G \right\}$ (its set of *subgroups*) by conjugation.

- The orbit $\mathcal{O}(H) = \left\{ gHg^{-1} \;\middle|\; g \in G \right\}$ is the **set of conjugate subgroups** of H.
  - This action is transitive iff all subgroups are conjugate.
- The fixed points Fix form the set of **normal subgroups** of G.
- The stabilizer $\mathrm{Stab}(H) = N_G(H)$ is the **normalizer** of H in G.
- The kernel is the intersection of all normalizers.

Corollary 2.11.9.
Given $H \leq G$, the number of conjugate subgroups is $[G : N_G(H)]$, i.e.

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

2.11.3 Left Translation on Cosets

Example 2.11.10 ***(?):*** For a fixed proper subgroup $H < G$, let G act on its cosets $X := G/H := \left\{ gH \;\middle|\; g \in G \right\}$ by left translation.

- The orbit $\mathcal{O}(xH) = G/H$, the entire set of cosets.
  - Note that this is a *transitive* action.
- The stabilizer $\mathrm{Stab}(xH) = xHx^{-1}$, a **conjugate subgroup** of H
- The fixed points form $\mathrm{Fix} = \emptyset$.
- The kernel of this action is $\bigcap_{g \in G} gHg^{-1}$, the intersection of all conjugates of H.

Proposition 2.11.11 ***(Application of translation action on cosets).***
If G is a finite group and $p := [G : H]$ is the smallest prime dividing $\#G$, then $H \trianglelefteq G$.

Proof (?).

- Let $\varphi : G \curvearrowright X := \{xH\}$, noting that $\#X = p$ and $\mathrm{Sym}(X) \cong S_p$.
- Then $K := \ker \varphi \subseteq H$.

- Since G is finite and $K \leq G$, we have $[G : K] = \#(G/K) = \#G/\#K$ so $\#(G/K)$ divides $\#G$.
- Since $G/K \cong K'$ is isomorphic to a subgroup of S_p, $\#(G/K)$ divides $\#S_p = p!$
- So $\#(G/K)$ divides $\gcd(\#G, p!)$, which is p since it was the minimal prime dividing $\#G$.
- p is prime, so if $\#G/K \neq 1$ we have $\#G/K = p$.
- Since $K \subset H$ and $[G : H] = p = [G : K]$, we have $K = H$.
- But $K = \ker \varphi \trianglelefteq G$, so $H \trianglelefteq G$.

■

Exercise 2.11.12 (?)
Prove Poincaré's theorem: if $H \leq G$ is finite index, then there exists an $N \trianglelefteq H$ where $[N : H] < n!$.

3 Sylow Theorems

Definition 3.0.1
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.

3.1 Sylow 1 (Cauchy for Prime Powers)

Theorem 3.1.1 *(Sylow 1).*

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

Slogan 3.1.2
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.

3.2 Sylow 2 (Sylows are Conjugate)

Theorem 3.2.1 ***(Sylow 2).***
All Sylow-p subgroups S_p are conjugate, i.e.

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

Corollary 3.2.2.

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

3.3 Sylow 3 (Numerical Constraints)

Theorem 3.3.1 ***(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.

3.4 Corollaries and Applications

Corollary 3.4.1.
By Sylow 3, p does not divide n_p.

Proposition 3.4.2.
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 $H := \cup_i H^i$ is maximal and thus a Sylow p-subgroup. ■

3.5 Proof of Sylow Theorems

3.6 Exercises

- Let G be a group of order p with v and e positive integers, p prime, $p > v$, and v is not a multiple of p. Show that G has a normal Sylow p-subgroup.

3.7 Automorphism Groups

Fact 3.7.1

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

3.8 Isomorphism Theorems

Theorem 3.8.1 ***(1st Isomorphism Theorem).***
If $\varphi : G \to H$ is a group morphism then
$$G/\ker\varphi \cong \mathrm{im}\,\varphi.$$
Note: for this to make sense, we also have

- $\ker\varphi \trianglelefteq G$

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

Corollary 3.8.2.
If $\varphi : G \to H$ is surjective then $H \cong G/\ker\varphi$.

Theorem 3.8.3 ***(Diamond Theorem / 2nd Isomorphism Theorem).***
If $S \leq G$ and $N \trianglelefteq G$, then

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

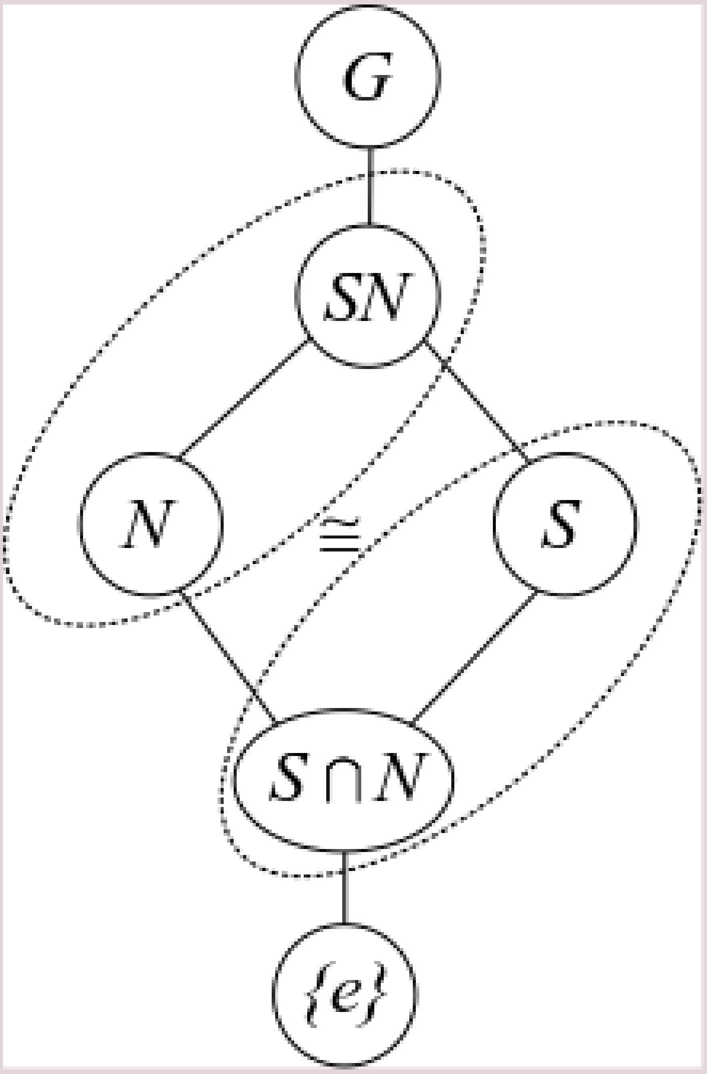


Figure 1: The 2nd “Diamond” Isomorphism Theorem

Remark 3.8.4: 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 3.8.5 ***(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 3.8.6 ***(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 3.8.7
$N \trianglelefteq G$ and $N \subseteq H < G \implies N \trianglelefteq H$.

3.9 Products

Proposition 3.9.1 ***(HK Subgroup Theorem).***
If $H, K \leq G$ and $H \leq N_G(K)$ (or $K \trianglelefteq G$) then $HK \leq G$ is a subgroup.

Theorem 3.9.2 ***(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 3.9.3 ***(Recognizing Direct Products).***
We have $G \cong H \times K$ when

1. $H, K \trianglelefteq G$
2. $G = HK$.
3. $H \cap K = \{e\} \subset G$

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

Proof (?).
With these conditions, the following map is an isomorphism:

$$\begin{aligned} \Gamma : H \times K &\to G \\ (h,k) &\mapsto hk. \end{aligned}$$

- This is a group morphism by condition (1):

$$\Gamma(h_1,k_1)\Gamma(h_2,k_2) := (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k_1)k_2 = (h_1h_2)(k_1k_2) := \Gamma((h_1,k_1)(h_2,k_2)).$$

- This is surjective by condition (2)
- This is injective by condition(3) and checking the kernel:

$$\ker\Gamma = \left\{(h,k) \;\middle|\; hk = 1_G,\, hk = 1_G\right\} \implies h = k^{-1} \implies hk \in K \cap H = \{1_G\}.$$

■

Theorem 3.9.4 ***(Recognizing Generalized Direct Products).***
We have $G \cong \prod_{i=1}^{n} H_i$ when

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

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

Theorem 3.9.5 ***(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

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

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

3.10 Classification: Finitely Generated Abelian Groups

Definition 3.10.1 (Invariant Factor Decomposition)
If G is a finitely generated abelian group, then there is a decomposition

$$G \cong \mathbb{Z}^r \times \prod_{k=1}^{m} \mathbb{Z}/n_k \quad \text{where } n_1 \mid \cdots \mid n_m,$$

where $r \in \mathbb{Z}^{\geq 0}$ is unique and the n_i are uniquely determined.

Definition 3.10.2 (Elementary Divisor Decomposition)
If G is a finitely generated abelian group, then there is a unique list of (not necessarily distinct) prime powers such that

$$G \cong \mathbb{Z}^r \times \prod_{k=1}^{m} \mathbb{Z}/p_k^{e_k},$$

where $r \in \mathbb{Z}^{\geq 0}$ is uniquely determined.

Proposition 3.10.3 ***(Converting between elementary divisors and invariant factors).***
Given any presentation of a group as a product of cyclic groups $G = \prod \mathbb{Z}_i/m_i$, with the m_i not necessarily distinct,

- Factor all of the m_i into prime powers, keeping the exponents intact.
- Organize into a table whose columns correspond to individual primes p_i.
  - Within an individual column for the prime p_k, write all terms of the form $p_k^{e_k}$ (with exponents intact)
  - Arrange the terms from lowest at the top to highest at the bottom. Push everything down so that the bottom-most rows are all filled out.
- For **elementary divisors**, just list out all of elements of the table individually, running across rows.
- For **invariant factors**, iterate a process of taking the largest of each prime power (i.e. the bottom row) at each step, deleting that row, and continuing in the same fashion.

Note: this sounds much more complicated than it actually is!

p_1	p_2	p_3	p_4
$p_1^{e_1}$		$p_3^{g_1}$	
$p_1^{e_2}$	$p_2^{f_1}$	$p_3^{g_2}$	
$p_1^{e_3}$	$p_2^{f_2}$	$p_3^{g_3}$	$p_4^{h_4}$

Example 3.10.4 ***(Abstract Example):***

- Elementary divisors: take columns.

$$\begin{aligned}&\mathbb{Z}/p_1^{e_1} \times \mathbb{Z}/p_1^{e_2} \times \mathbb{Z}/p_1^{e_3} \\ &\quad \times \mathbb{Z}/p_2^{f_1} \times \mathbb{Z}/p_2^{f_2} \\ &\quad \times \mathbb{Z}/p_3^{g_1} \times \mathbb{Z}/p_3^{g_2} \times \mathbb{Z}/p_3^{g_3} \\ &\quad \times \mathbb{Z}/p_4^{h_4}.\end{aligned}$$

- Invariant factors: take rows (grouped by CRT)

$$\begin{aligned}&\mathbb{Z}/\left(p_1^{e_3} p_2^{f_2} p_3^{g_3} p_4^{h_4}\right) \\ &\quad \times \mathbb{Z}/\left(p_1^{e_2} p_2^{f_1} p_3^{g_2}\right) \\ &\quad \times \mathbb{Z}/\left(p_1^{e_1} p_3^{g_1}\right).\end{aligned}$$

Example 3.10.5 ***(of putting a group in invariant factor form):***

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

I'll use a shortcut for the table: instead of listing columns, I just list the prime powers for a single p in increasing order in the same cell. Then just always take the largest prime power in each cell at each stage:

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

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

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

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

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

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

and thus the invariant factor form is

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

Example 3.10.6:

$$G \coloneqq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{5^2\cdot 7}$$

Make the table by factoring the order of each cyclic piece, being careful not to combine terms that come from distinct summands (e.g. not combining the two copies of 2^1), and to keep exponents from factorizations intact as a single term (e.g. the 2^3):

2	5	7
2		
2		
2^3	5^2	7

Reading across rows from bottom to top (and using CRT to merge everything within a row) yields invariant factors on the LHS below. Reading down columns, left to right (merging nothing) yields elementary divisors on the RHS:

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

Proposition 3.10.7 ***(Number of abelian groups is given by products of partition numbers).***
If $\#G \coloneqq n = \prod_{k=1}^{m} p_k^{e_k}$, then there are exactly $\prod_{k=1}^{m} P(e_k)$ abelian groups of order n, where P is the integer partition function.

Example 3.10.8 ***(of an integer partition):*** One can compute $P(6) = 11$, where all of the partitions are given by

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

Remark 3.10.9: In practice, it is easy to list all of the partitions out for a given n, but it's also useful to have a systematic way to generate them and actually check that you have them all.

Proposition 3.10.10 ***(Formula for partitions).***
There is a recurrence relation

$$P_k(n) = P_k(n-k) + P_{k-1}(n-1),$$

which follows from the fact that one can obtain a partition of n with k parts by either

- Taking a partition of $n-k$ into k parts and adding 1 to each part, e.g. $[1,1,1,3] \mapsto [2,2,2,4]$
- Taking a partition of $n-1$ into $k-1$ parts and adding a new standalone part 1, e.g. $[1,1,2,5] \mapsto [1,1,2,5,1]$.

Summing over k yields the following, which can be recursed:

$$\begin{aligned}
P(n) &= \sum_{k=1}^{n} P_k(n-k) + P(n-1)\\
&= \sum_{k=1}^{n} P_k(n-k) + \sum_{k=1}^{n-1} P_k(n-1-k) + P(n-2)\\
&= \cdots,
\end{aligned}$$

where $P_k(m) = 0$ for $k > m$ and $P_m(m) = 1$.

Example 3.10.11 ***(?):*** One can compute that $P(5) = 7$, and the formula recovers this:

$$\begin{aligned}
P(5) &= \sum_{k=1}^{5} P_k(5-k) + P(4) \\
&= (P_1(4) + P_2(3)) + P(4) \\
&= (P_1(4) + P_2(3)) + (P_1(3) + P_2(2)) + P(3) \\
&= (P_1(4) + P_2(3)) + (P_1(3) + P_2(2)) + (P_1(2)) + P(2) \\
&= (P_1(4) + P_2(3)) + (P_1(3) + P_2(2)) + (P_1(2)) + (P_1(1) + P(1)) \\
&= (1+1) + (1+1) + (1) + (1+1) \\
&= 7.
\end{aligned}$$

Note that you could just stop at the third line, since $P(3) = 3$ is easy to enumerate: $[1,1,1], [1,2], [3]$.

Example 3.10.12 ***(Applying this to classifying groups):*** Suppose $\#G = n = p^3q^4$. Compute that $p(3) = 3$ and $p(4) = 5$, so there should be 15 abelian groups of this order. Enumerate the partitions:

- For 3: $[1,1,1], [1,2], [3]$
- For 4: $[1,1,1,1], [1,2,1], [1,3], [2,2], [4]$

Now for every distinct pair taking one from the first line and one from the second, we get a group of that order. A partition of m of the form $[a, b, c, \cdots]$ contributes a group of the form $\mathbb{Z}_{m^a} \times \mathbb{Z}_{m^b} \times \mathbb{Z}_{m^c} \cdots$.

Crossing $[1,1,1]$ with everything:

- $(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p) \times (\mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_q) \mapsfrom [1,1,1] \times [1,1,1,1]$
- $(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p) \times \left(\mathbb{Z}_q \times \mathbb{Z}_{q^2} \times \mathbb{Z}_q\right) \mapsfrom [1,1,1] \times [1,2,1]$
- $(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p) \times \left(\mathbb{Z}_q \times \mathbb{Z}_{q^3}\right) \mapsfrom [1,1,1] \times [1,3]$
- $(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p) \times \left(\mathbb{Z}_{q^2} \times \mathbb{Z}_{q^2}\right) \mapsfrom [1,1,1] \times [2,2]$
- $(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p) \times \mathbb{Z}_{q^4} \mapsfrom [1,1,1] \times [4]$

Crossing $[1,2]$ with everything:

- $\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right) \times (\mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_q) \mapsfrom [1,2] \times [1,1,1,1]$
- $\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right) \times \left(\mathbb{Z}_q \times \mathbb{Z}_{q^2} \times \mathbb{Z}_q\right) \mapsfrom [1,2] \times [1,2,1]$
- $\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right) \times \left(\mathbb{Z}_q \times \mathbb{Z}_{q^3}\right) \mapsfrom [1,2] \times [1,3]$
- $\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right) \times \left(\mathbb{Z}_{q^2} \times \mathbb{Z}_{q^2}\right) \mapsfrom [1,2] \times [2,2]$
- $\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right) \times \mathbb{Z}_{q^4} \mapsfrom [1,2] \times [4]$

And so on!

3.11 Classification: Groups of Special Orders

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

- Keith Conrad: Classifying Groups of Order 12
- Order pqr: ?
- Order p^2q: ?

Proposition 3.11.1 ***(Classification of groups of order*** p***).***
Every group G of prime order $p \geq 2$ is cyclic and thus isomorphic to $\mathbb{Z}/p$.
Supposing that $g \neq e$, it generates a cyclic subgroup $H := \langle g \rangle \leq G$ of order dividing p by Lagrange. Since $g \neq e$, $\#H = p = \#G$.

Proposition 3.11.2 ***(Classification of groups of order*** p^2***).***
Every group G of order p^2 is abelian, and thus isomorphic to either $\mathbb{Z}/p^2$ or $(\mathbb{Z}/p)^2$.
Quotient by the center to get $m := \#G/Z(G) \in \left\{1, p, p^2\right\}$

- Since G is a p-group, G has nontrivial center, so $m \neq 1$
- If $m = p$, then $G/Z(G)$ is cyclic and thus G is abelian by the $G/Z(G)$ theorem.
- If $m = p^2$, $Z(G) = G$ and G is abelian, done.

Proposition 3.11.3 ***(Classification of groups of order*** pq***).***
If G is a group of order pq where without loss of generality $q < p$, then

1. If $q \nmid p - 1$ then $G \cong S_p \times S_q \cong \mathbb{Z}/p \times \mathbb{Z}/q \cong \mathbb{Z}/pq$
2. If $q \mid p - 1$ then $G \cong S_q \rtimes_\psi S_p$ where $S_p \trianglelefteq G$ and $\psi : S_q \to \operatorname{Aut}(S_p)$, and G has a presentation

$$G \cong \left\langle a, b \;\middle|\; a^p, b^q, bab^{-1} = a^\ell \right\rangle$$

$$\ell \not\equiv 1 \pmod{p} \qquad\qquad \ell^q \equiv 1 \pmod{p}.$$

Proof (of pq *theorem, case 1).*

- Suppose $q < p$.
- Apply the Sylow theorems to p:
  - $n_p \cong 1 \pmod{p} \implies n_p \in \{1, p+1, 2p+1, \cdots\}$.
  - $n_p \mid q \implies n_p \in \{1, q\}$.
  - Since $1 < q < p < p+1$, this forces $n_p = 1$
- Suppose $q \nmid p - 1$ and apply the Sylow theorems to q:
  - $n_q \equiv 1 \pmod{q} \implies n_q \in \{1, q+1, 2q+1, \cdots\}$

  - $n_q \mid p \implies n_q \in \{1, p\}$
  - Now note that if $n_q \neq 1$, then $n_q = p$ and p is of the form $kq + 1$ for some k.
  - **Use of assumption**: then $p = kq + 1 \iff p - 1 = kq \iff q \mid p - 1$, which is precisely what we assumed is *not* the case.

- So $n_p = n_q = 1$ and $S_p, S_q \trianglelefteq G$.
- Apply recognition of direct products:

  - $S_p, S_q \leq G$: check.
  - $S_p, S_q \trianglelefteq G$: check.
  - $S_p \cap S_q = \{e\}$: check, because they are coprime order.
  - $S_p S_q = G$: follows from a counting argument:

$$\#S_p S_q = \frac{\#S_p \#S_q}{\#\left(S_p \cap S_q\right)} = \frac{pq}{1} = \#G.$$

If G is finite, then $AB \leq G$ with $\#AB = \#G$ implies $AB = G$.

■

Proof (of pq theorem, case 2). • Suppose $q \mid p - 1$, the previous argument for S_p works, but the argument for S_q doesn't, so we get a semidirect product.

- Work up to isomorphism:

$$S_p \cong \mathbb{Z}/p = \left\langle a \;\middle|\; a^p \right\rangle \trianglelefteq G$$

$$S_q \cong \mathbb{Z}/q = \left\langle b \;\middle|\; b^q \right\rangle \leq G.$$

- We have

$$G \cong \mathbb{Z}/q \rtimes_\psi \mathbb{Z}/p \qquad \psi : \mathbb{Z}/q \to \operatorname{Aut}\left(\mathbb{Z}/p\right)$$

$$\implies G \cong \left\langle a, b \;\middle|\; a^p, b^q,\ aba^{-1} = \psi(b) = b^\ell \right\rangle \qquad \text{for some } \ell.$$

  - Since $\mathbb{Z}/q$ is cyclic, such a morphism is determined by the image of the generator $[1]_q \in \mathbb{Z}/q$.
  - Note that $[1]_q \mapsto \mathrm{id}_{\mathbb{Z}/p}$ is such a morphism, and yields the direct product again.

- Identify $\operatorname{Aut}(\mathbb{Z}/p) \cong \left((\mathbb{Z}/p)^\times, \times\right) \cong (\mathbb{Z}/(p-1), +)$.
- So we need to classify morphisms

$$\psi : \mathbb{Z}/q \to \mathbb{Z}/(p-1).$$

  - Consider $\operatorname{im} \psi \leq \mathbb{Z}/(p-1)$.
  - Sending $[1]_q$ to the identity in $\operatorname{Aut}(\mathbb{Z}/p)$ yields the direct product again, so pick nontrivial morphisms.
  - Since $\# \operatorname{im} \psi \mid q$ which is prime, its order is equal to q.

  - Since $q \mid p-1$ and $\mathbb{Z}/(p-1)$ is cyclic of order $p-1$, by Cauchy's theorem there is a unique subgroup of order q, say $C_q \leq \mathbb{Z}(p-1)$
  - We can send $[1]_q$ to $[\alpha]_{p-1} \in \mathbb{Z}/(p-1)$ where α is any generator of C_q, of which there are $\varphi(q) = q-1$ nontrivial choices.

- Thus there are $q-1$ distinct nontrivial choices for the action $\psi : \mathbb{Z}/q \to \mathbb{Z}/(p-1)$.

Claim: All choices yield isomorphic semidirect products.

- Use that $G := A \rtimes_\psi N$ with $\psi : A \to \operatorname{Aut}(N)$ is an $\operatorname{Aut}(N)$ and $\operatorname{Aut}(A)$ module, where $f \in \operatorname{Aut}(N)$ and $\pi \in \operatorname{Aut}(A)$ act in the following ways:

$$\begin{aligned} \pi \curvearrowright A \rtimes_\psi N &= A \rtimes_{\psi \circ \pi} N \\ f \curvearrowright A \rtimes_\psi N &= A \rtimes_{\gamma_f \circ \psi} N. \end{aligned}$$

  where

$$\begin{aligned} \gamma_f : \operatorname{Aut}(N) &\to \operatorname{Aut}(N) \\ \psi &\mapsto f \circ \psi \circ f^{-1}. \end{aligned}$$

  - These actions preserve the group isomorphism type of G

- However, since $C_q \leq \mathbb{Z}/(p-1)$ and $\operatorname{Aut}(C_q) \cong \mathbb{Z}/(q-1)$, there are exactly $q-1$ automorphisms of the image C_q, say $\{\pi_k\}_{k=1}^{q-1}$.
- So $\psi \circ \pi_k : \mathbb{Z}/q \to \mathbb{Z}/(p-1)$ for $1 \leq k \leq q-1$ yields $q-1$ distinct actions, and we're done.

■

Proposition 3.11.4 ***(PQR Theorem).***
If $|G| = pqr$ where $p < q < r$ are distinct primes then G is solvable.

3.12 Series of Groups

Definition 3.12.1 (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 3.12.2 (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 3.12.3 (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 3.12.4 ***(Jordan-Holder).***
Any two composition series of a group have the same length and isomorphic composition factors (up to permutation).

Definition 3.12.5 (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 3.12.6.
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 3.12.7 (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 adjoint map $[-, G]$, if this terminates then the map is nilpotent, so call G nilpotent!

Definition 3.12.8 (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 centers".

Definition 3.12.9 (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 3.12.10 (Solvable)
A group G is **solvable** iff G has a terminating normal series with abelian composition factors, i.e.

$$G \coloneqq G_n > G_{n-1} > \cdots > G_2 > G_1 \coloneqq \{e\} \qquad \text{with } G^i/G^{i+1} \text{ abelian for all } i.$$

Remark 3.12.11: If $G = \mathrm{Gal}(L/K)$ is a Galois group corresponding to a polynomial f, then G is solvable as a group iff f is solvable in radicals: there is a tower of extensions $K = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m = L$ where

1. $F_i = F_{i-1}(\alpha_i)$ where $\alpha_i^{m_i} \in F_{i-1}$ for some power $m_i \in \mathbb{Z}^{\geq 0}$, and
2. $F_m \supseteq \mathrm{SF}(f)$ contains a splitting field for f.

Theorem 3.12.12 ***(Characterization of Solvable).***
A group G is solvable iff its derived series terminates.

Theorem 3.12.13 ***(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.

4 | Ring Theory

Proposition 4.0.1 ***(Ideal Operations).***

- $I + J = \left\{ i + j \;\middle|\; i \in I, j \in J \right\} = \langle I, J \rangle$ is the smallest ideal containing I and J.
- $IJ = \left\{ \sum_{k \leq N} x_k y_k \;\middle|\; x_k \in I, y_k \in J, N \in \mathbb{Z}^{\geq 0} \right\}$ is the ideal generated by all finite sums of products.
- $I \cap J$ is an ideal, $I \cup J$ is generally **not** an ideal
- Ideals are *comaximal* if $I + J = \langle 1 \rangle$.
- If $I + J = \langle 1 \rangle$ then $I \cap J = IJ$.

4.1 Isomorphism Theorems

Remark 4.1.1: These are all basically the same for modules.

Proposition 4.1.2 ***(First Isomorphism Theorem).***
For any ring morphism $f : A \to B$ there is SES of rings

$$0 \to \ker f \to A \to \operatorname{im}(f) \to 0,$$

and thus $A/\ker f \cong \operatorname{im} f$. If f is surjective, then $A/\ker f \cong B$.
More traditionally stated:

- $\ker \varphi \in \operatorname{Id}(A)$
- $\operatorname{im} \varphi \leq B$ is a subring (not necessarily an ideal)
- $R/\ker \varphi \cong \operatorname{im} \varphi$.

Proposition 4.1.3 ***(Second Isomorphism Theorem).***
Let $R \in \mathsf{Ring}, S \leq R, I \in \mathrm{Id}(R)$, then there is an isomorphism:

$$\frac{S+I}{I} \xrightarrow{\sim} \frac{S}{S \cap I}.$$

Where it's also true that this statement makes sense:

- $S + I \leq R$ is a subring.
- $S \cap I \trianglelefteq S$

Proposition 4.1.4 ***(Third Isomorphism Theorem).***
For $I \in \mathrm{Id}(R)$, the canonical quotient map $\varphi : R \to R/I$ induces a bijective correspondence:

$$\begin{aligned} \left\{ {\scriptstyle J \in \mathrm{Id}(R)} \;\middle|\; {\scriptstyle J \supseteq I} \right\} &\rightleftharpoons \mathrm{Id}(R/I) \\ J := \varphi^{-1}(\overline{J}) &\leftarrow\!\shortmid \overline{J} \\ J &\mapsto \overline{J} := \varphi(J), \end{aligned}$$

where $\varphi : R \to R/I$ is the canonical quotient morphism.
More traditionally:

- If $S, I \in \mathrm{Id}(R)$ with S containing I then
$$S/I \leq R/I.$$
- Every ideal in $\mathrm{Id}(R/I)$ is of the form $\overline{S} := S/I$ for some $S \in \mathrm{Id}(R)$ containing I.
- If $I, J \in \mathrm{Id}(R)$ with $I \subseteq J \subseteq R$ then there is an isomorphism
$$\frac{R/I}{J/I} \xrightarrow{\sim} \frac{R}{J}.$$

Moreover, $A \leq R$ is a subring containing I iff $A/I \in \mathrm{Id}(R/I)$.

Exercise 4.1.5 (?)
Show that if $J \in \mathrm{Id}(R)$ (with $J \supseteq I$) is radical/prime/maximal iff $\overline{J} \in \mathrm{Id}(R/I)$ is radical/prime/maximal.

4.2 Important Techniques

Proposition 4.2.1 ***(Fields are simple).***
$R \in \mathsf{Field} \iff \mathrm{Id}(R) = \{0, R\}$.

Proof (?).
$\implies$: If $0 \neq x \in I \trianglelefteq R$, using that $R^\bullet = R^\times$, x is a unit. So $x^{-1} \in R$, and $xx^{-1} := 1 \in I$ so $I = R$.
$\impliedby$: Let $x \in R^\bullet$, then $Rx = R$ so $1 \in Rx$ and $1 = rx$ for some $r \in R$. This forces $x = r^{-1}$. ■

Proposition 4.2.2 ***(Showing ideals are maximal/prime with quotients).***

- $R/\mathfrak{m}$ is a field $\iff$ $\mathfrak{m} \in \operatorname{mSpec}(R)$ is maximal.
- $R/\mathfrak{p}$ is an integral domain $\iff$ $\mathfrak{p} \in \operatorname{Spec}(R)$ is prime.
- R/J is reduced $\iff$ J is radical.

Proof (of 1).
Use the ideal correspondence theorem: $\operatorname{Id}(R/\mathfrak{m})$ are ideals of R containing $\mathfrak{m}$:

$$\begin{aligned} & R/\mathfrak{m} \in \mathsf{Field} \\ \iff & \nexists J/\mathfrak{m} \in \operatorname{Id}(R/\mathfrak{m})^\bullet \text{ such that } J \in \operatorname{Id}(R) \\ \iff & \nexists \mathfrak{m} \subsetneq J \subsetneq R \\ \iff & J \in \operatorname{mSpec}(R). \end{aligned}$$

■

Proof (of 2).
$\impliedby$: Show $xy = 0$ with $x \neq 0$ forces $y = 0$. Let $x, y \in \mathfrak{p} \in \operatorname{Spec} R$, so $x = a + I, y = b + I$ for some $a, b \in R$. If $xy = 0 \pmod{\mathfrak{p}}$ with $y \neq 0 \pmod{\mathfrak{p}}$, we can check

$$xy = (a + \mathfrak{p})(b + \mathfrak{p}) := (ab) + \mathfrak{p} = 0 + \mathfrak{p} \implies ab \in \mathfrak{p}.$$

Since $\mathfrak{p}$ is prime and $x \neq 0 \implies a \notin \mathfrak{p}$, so $b \in \mathfrak{p}$. But then

$$y := b + \mathfrak{p} = 0 + \mathfrak{p} = 0 \pmod{\mathfrak{p}}.$$

$\implies$: Let $a, b \in R$ with $xy \in \mathfrak{p}$, we want to show that if $x \notin \mathfrak{p}$ then $y \in \mathfrak{p}$. Note $x \notin \mathfrak{p} \iff x \cong 0 \pmod{\mathfrak{p}}$. Setting $x := a + \mathfrak{p}, y := b + \mathfrak{p}$ yields

$$xy := (a + \mathfrak{p})(b + \mathfrak{p}) := ab + \mathfrak{p} = 0 \pmod{\mathfrak{p}}.$$

Since $R/\mathfrak{p}$ is a domain, assuming $x \neq 0 \pmod{\mathfrak{p}}$ we have $y = 0 \pmod{\mathfrak{p}}$, so $y \in \mathfrak{p}$. ■

Remark 4.2.3: Note that this yields a quick proof that $\operatorname{mSpec} R \subseteq \operatorname{Spec} R$, using that $\mathsf{Field} \leq \mathsf{IntDomain}$:

$$I \text{ maximal} \iff R/I \in \mathsf{Field} \implies R/I \in \mathsf{IntDomain} \iff I \text{ prime}.$$

Fact 4.2.4
If $\mathfrak{m}$ is maximal and $x \in R \setminus \mathfrak{m}$ then $\mathfrak{m} + Rx = R = \langle 1 \rangle$.

Fact 4.2.5
The binomial expansion works in any ring:

$$(a+b)^n = \sum_{k\leq n} \binom{n}{k} a^k b^{n-k}.$$

This is useful when considering nilpotents or radicals.

4.3 Undergrad Review

Remark 4.3.1: Notation:

- $\langle a \rangle := Ra := \left\{ ra \,\middle|\, r \in R \right\}$ is the ideal generated by a single element.
- $R = \langle 1 \rangle$ is equivalently the ideal generated by 1.

4.3.1 Basics

Definition 4.3.2 (Ring)
A **ring** is a triple $(R, +, \cdot) \in \mathsf{CRing}$ such that

- $(R, +) \in \mathsf{AbGrp}$,
- $(R, \cdot) \in \mathsf{Mon}$
- Distributivity: $a(b+c) = ab + ac$.

Example 4.3.3 ***(of rings):*** Some of the most important examples of rings:

- The usual suspects: $\mathbb{Z}, \mathbb{Q}$
  - Their analogs: number fields $K := \mathbb{Q}(\zeta)$, their rings of integers $\mathbb{Z}_K$ or $\mathcal{O}_K$,
- Gaussian integers $\mathbb{Z}(i)$
- Fields $k = \mathbb{F}_{p^n}, \mathbb{R}$
- Fraction fields of rings $\operatorname{ff}(R)$, e.g. $\operatorname{ff}(\mathbb{Z}) = \mathbb{Q}$.
- Polynomial rings $R[x_1, x_2, \cdots, x_n]$, particularly for $R = k$ a field
- Power series rings $R[x_1, x_2, \cdots, x_n]$.
  - Formal power series rings $R[[x_1, x_2, \cdots, x_n]]$.
- $\mathbb{Z}_p := \left\{ a/b \,\middle|\, p \nmid b \right\}$ the ring of p-adic integers
- Rings of germs, e.g. $C^\infty(X, Y)$ where $f \sim g$ iff there exists some $U \subseteq X$ with $f|_U = g|_U$.

Definition 4.3.4 (Ring Morphism)
A morphism $f \in \mathsf{CRing}(X, Y)$ satisfies:

- $f(1_X) = 1_Y$
- $f(a(b + c)) = f(a)f(b) + f(a)f(c)$

Remark 4.3.5: Important notes:

- $\ker f := f^{-1}(\{0\})$.
- A bijective ring morphisms is automatically an isomorphism in CRing.
- $\ker f \trianglelefteq X$ is an ideal, but $\operatorname{im} f \leq Y$ is only a subring in general.
- For any ideal $I \trianglelefteq R$ there is a quotient map $R \to R/I$, it's useful to write cosets as $a + I$.
- For quotients, $x \equiv y \pmod{I} \iff x - y \in I$.

Definition 4.3.6 (Ideal)
An **ideal** $I \trianglelefteq R$ is a subset where $(I, +) \leq (R, +) \in \mathsf{Grp}$ is a subgroup and for $x \in R, i \in I$, $xi \in I$. Equivalently,

- $RI \subseteq I$
- $I + I \subseteq I$

Note that 0 is in every ideal.

Definition 4.3.7 (Characteristic)
Using that every ring has a $\mathbb{Z}$-Mod structure, the **characteristic** of a ring R is the smallest n such that $n \curvearrowright 1_R = 0_R$, i.e. $\displaystyle\sum_{i=1}^{n} 1_R = 0_R$.

4.3.2 Elements

Definition 4.3.8 (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 4.3.9 (Units)
An element $r \in R$ is a **unit** if $r \mid 1$: there exists an $s \in R$ such that $rs = sr = 1$. Then $r^{-1} := s$ is uniquely determined, and the set of units $(R^\times, \cdot) \in \mathsf{AbGrp}$ forms a group.

Definition 4.3.10 (Irreducible Element)
An element $r \in R$ is **irreducible** iff

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

Definition 4.3.11 (Prime Element)
An element $p \in R$ is **prime** iff

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

Fact 4.3.12
If R is an integral domain, prime $\implies$ irreducible. If R is a UFD, then prime $\iff$ irreducible.

Definition 4.3.13 (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 $b \mid a$.

4.3.3 Ideals

Example 4.3.14 ***(of specs):***

- $\operatorname{Id}(\mathbb{Z}) = \left\{ \langle m \rangle \;\middle|\; m \in \mathbb{Z}^{\geq 0} \right\}$
- $\operatorname{mSpec} \mathbb{Z} = \left\{ \langle p \rangle \;\middle|\; p \neq 0 \text{ is prime} \right\}$
- $\operatorname{Spec} \mathbb{Z} = \operatorname{mSpec} \mathbb{Z} \cup \{\langle 0 \rangle\}$.
- For k a field and $f \in k[x_1, \cdots, x_n]$ irreducible, $\langle f \rangle \in \operatorname{Spec} k[x_1, \cdots, x_n]$.
  - $\mathfrak{m} := \left\{ f = \sum_I a_I x^I \in k[x_1, \cdots, x_n] \;\middle|\; a_0 = 0 \right\} \in \operatorname{mSpec} k[x_1, \cdots, x_n]$ (i.e. this is the ideal of polynomials with no constant term).

Proposition 4.3.15 ***(Proper ideals contain no units).***
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 4.3.16.
If $I_1 \subseteq I_2 \subseteq \cdots$ are ideals then $\cup_j I_j$ is an ideal.

Definition 4.3.17 (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 4.3.18 (Prime Ideal)
$\mathfrak{p}$ is a **prime** ideal $\iff$

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

Proposition 4.3.19 ***(Prime implies irreducible for UFDs).***
In R a UFD, an element $r \in R$ is prime $\iff$ r is irreducible.

Example 4.3.20 ***(of why the converse doesn't hold):*** 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.

Definition 4.3.21 (Prime Spectrum)
The **prime spectrum** (or just the **spectrum**) of R is defined as

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

Definition 4.3.22 (Maximal Ideal)
An ideal $\mathfrak{m}$ is **maximal** iff whenever $I \trianglelefteq R$ with $I \supseteq \mathfrak{m}$ then $I = R$.

Example 4.3.23 ***(Some counterexamples):***

- A non-maximal, non-prime ideal: $\left\langle x^4 + 2x^2 + 1 \right\rangle \trianglelefteq \mathbb{C}[x]$
- An ideal that is both prime and maximal: $\langle f \rangle$ for any $f \in \mathbb{Q}[x]^{\mathrm{irr}}$
- A prime ideal that is not maximal: $\langle x - c \rangle \in \mathbb{R}[x]$.

Definition 4.3.24 (Max Spectrum)
The **max spectrum** of R is defined as

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

Example 4.3.25 ***(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 4.3.26: Maximal ideals of $R[x]$ are of the form $I = (x - a_i)$ for some $a_i \in R$.

4.4 Types of Rings

Definition 4.4.1 (Division ring or skew field)
A **division ring** is any (potentially noncommutative) ring R for which $R \setminus \{0\} \subset \mathbb{R}^\times$, i.e. every nonzero element is a unit and thus has a multiplicative inverse.

Definition 4.4.2 (Zero Divisor)
An element $r \in R$ is a **zero-divisor** iff there exists an $a \in R \setminus \{0\}$ such that $ar = ra = 0$,

i.e. $r \mid 0$. Equivalently, the map

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

fails to be injective.

Definition 4.4.3 (Integral Domain)
A ring is an **integral domain** if and only if it has no nonzero zero divisors:

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

Example 4.4.4 ***(of integral domains):*** Examples of integral domains: $\mathbb{Z}, k[x_1, x_2, \cdots, x_n]$. Non-examples: $\mathbb{Z}/6, \mathrm{Mat}(2 \times 2; k)$

Definition 4.4.5 (Field)
A **field** is a commutative division ring, i.e. every nonzero element is a uni, i.e. every nonzero element is a unit

Exercise 4.4.6 (?)
Show that TFAE:

- $A \in \mathsf{Field}$
- A is a simple ring, so $\mathrm{Id}(A) = \{0, A\}$.
- If $B \in \mathsf{Field}$ is nonzero then every ring morphism $A \to B$ is injective.

Remark 4.4.7: Every field is an integral domain, but e.g. $\mathbb{Z}$ is an integral domain that is not a field.

Definition 4.4.8 (Principal Ideal)
An ideal $I \trianglelefteq R$ if **principal** if there exists an $a \in R$ such that $I = \langle a \rangle$, i.e. $I = Ra$.

Definition 4.4.9 (Principal Ideal Domain)
A ring R is a **principal ideal domain** iff every ideal is principal.

Exercise 4.4.10 (?)
Show that if R is a PID then $\operatorname{Spec} R \subseteq \operatorname{mSpec} R$.

Definition 4.4.11 (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.

Definition 4.4.12 (Noetherian)
A ring R is **Noetherian** if the ACC holds: every ascending chain of ideals $I_1 \leq I_2 \cdots$ stabilizes in the sense that there exists some N such that $I_N = I_{N+1} = \cdots$.

Definition 4.4.13 (Reduced Ring)
A ring R is **reduced** if R contains no nonzero nilpotent elements.

Definition 4.4.14 (Local Ring)
A ring R is **local** iff it contains a unique maximal ideal $\mathfrak{m}$, so $\operatorname{mSpec} R = \{0, \mathfrak{m}\}$. As a consequence, there is a uniquely associated **residue field** $\kappa := R/\mathfrak{m}$.

Exercise 4.4.15 (?)
Show that if R is a nonzero ring where every element is either a unit or nilpotent, then R is local.

Exercise 4.4.16 (?)
Show that if $p \in \operatorname{Spec} R$ then $R\left[p^{-1}\right]$ is local.

Exercise 4.4.17 (?)
Suppose $\mathfrak{m} \in \operatorname{mSpec} R$ is a proper maximal ideal. Show that under either of the following two conditions, R is local:

- $R \setminus \mathfrak{m} \subseteq R^\times$, so every element of $R \setminus \mathfrak{m}$ is a unit, or
- $1 + \mathfrak{m} \subseteq R^\times$

Solution:
- Sketch: $\mathfrak{m}$ must contain every non-unit.
  - If $I \neq R$ then I contains no units, so $I \subseteq N := R \setminus R^\times$, i.e. I is contained in the non-units. But $N \subseteq \mathfrak{m}$ since no element of $\mathfrak{m}$ is a unit and no element of $R \setminus \mathfrak{m}$ is a non-unit.
- Sketch: show that every $r \in R \setminus \mathfrak{m}$ is a unit and apply the first part.
  - If $r \in R \setminus \mathfrak{m}$ then $\langle r, \mathfrak{m} \rangle = R = \langle 1 \rangle$ so $rt + m = 1$ for some $t \in R, m \in \mathfrak{m}$, so $rt = 1 - m \in 1 + \mathfrak{m} \subseteq R^\times$ by assumption. Now apply (1).

Definition 4.4.18 (Dedekind Domains)
A **Dedekind domain** is an integral domain for which the monoid $\operatorname{Id}(R)$ of nonzero ideals of R satisfies unique factorization: every ideal can be decomposed uniquely into a product of prime ideals.

Exercise 4.4.19 (?)
Show that a Dedekind domain R is a PID iff R is a UFD.

Definition 4.4.20 (Valuation Ring)
A **valuation ring** is an integral domain R such that for every $x \in \operatorname{ff}(R)$, $x \in R$ or $x^{-1} \in R$.

Definition 4.4.21 (Discrete Valuation Rings)
A **discrete valuation ring** or **DVR** is a local PID with a *unique* maximal ideal.

Definition 4.4.22 (Regular ring)
A commutative ring R is **regular** if R is Noetherian and for every $p \in \operatorname{Spec} R$ the localization $R\left[p^{-1}\right]$ is a *regular local ring*: it has a maximal ideal $\mathfrak{m}$ which admits a minimal generating set of n elements where n is the Krull dimension of $R\left[p^{-1}\right]$.

Remark 4.4.23: Motivation: if $R = \mathcal{O}_{X,x}$ is the ring of germs at x of an algebraic variety X, then R is regular iff X is nonsingular at x.

Definition 4.4.24 (Gorenstein Rings)
A commutative Noetherian ring R is **Gorenstein** iff R viewed as an R-module has finite injective dimension.

Example 4.4.25 ***(Why care about Gorenstein rings?):*** If $R \in \mathsf{gr\,Alg}_{/k}$ with $\dim_k R < \infty$, then R decomposes as $R = R_0 \oplus R_1 \oplus \cdots R_n$ with $R_0 := k$, and R is Gorenstein iff R satisfies "Poincaré duality": $\dim_k R_0 = \dim_k R_m = 1$ and there is a perfect pairing $R_i \otimes_k R_{n-j} \to R_n$.

4.5 Comparing and Transporting Ring Types

Proposition 4.5.1 ***(Big chain of inclusions).***
Fields $\subset$ Euclidean domains $\subset$ PIDs $\subset$ UFDs $\subset$ Integral Domains $\subset$ Rings

Prove inclusions

Proposition 4.5.2 ***(PID implies UFD).***
If R is a PID, then every element in R has a unique prime factorization.

Example 4.5.3 ***(showing these inclusions are strict):***

- 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: $\mathbb{Z}\left[\dfrac{1+\sqrt{-19}}{2}\right]$.
  - *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 4.5.4 ***(Polynomial rings over fields have division).***
If $\mathbb{F}$ a field then $\mathbb{F}[x]$ is a Euclidean domain.

Proposition 4.5.5 ***(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 $\iff$ $\mathbb{F}[x]$ 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.

Example 4.5.6 ***(?):*** A polynomial ring over a PID is not necessarily a PID: take $\langle 2, x\rangle \trianglelefteq \mathbb{Z}[x]$.

4.6 Radicals

Definition 4.6.1 (Radical of an Ideal)
For an ideal $I \trianglelefteq R$, the **radical**

$$\sqrt{I} := \left\{ r \in R \;\middle|\; r^n \in I \text{ for some } n \geq 0 \right\},$$

so $x^n \in I \implies x \in \sqrt{I}$.

Remark 4.6.2: In general, "radical" refers to "bad elements" of some type to be quotiented out, not necessarily $\sqrt{-}$.

Definition 4.6.3 (Radical Ideal)
An ideal is **radical** iff $\sqrt{I} = I$.

Definition 4.6.4 (Nilpotent)
An element $r \in R$ is **nilpotent** if $r^n = 0$ for some $n \in \mathbb{Z}^{\geq 0}$.

Definition 4.6.5 (Nilradical)
The **nilradical** of $R \in \mathsf{CRing}$ is

$$\sqrt{0_R} := \left\{ x \in R \;\middle|\; x \text{ is nilpotent} \right\} = \sqrt{0}.$$

Exercise 4.6.6 (Quotient by nilradical is reduced)
Show $\sqrt{0_R} \trianglelefteq R$ is an ideal and $A/\sqrt{0_R}$ is reduced.

Solution:

- $R\sqrt{0_R} \subseteq R$: For r nilpotent of order n and $x \in R$, xr is nilpotent since
$$(xr)^n = (xr)(xr)\cdots(xr) = x^n r^n = x^n 0 = 0.$$
- $R^2 \subseteq R$, for $r, s \in \sqrt{0_R}$ write $r^n = s^m = 0$, then
$$(r+s)^N = \sum_{k \geq 0} \binom{N}{k} r^k s^{N-k},$$
so just choose N large enough so that either $k > n$ or $N - k > m$ always holds, e.g. $N := n + m - 1$.
- $R/\sqrt{0_R}$ has no nonzero nilpotents: Take $\bar{r} \in R/\sqrt{0_R}$ for some $r \in R$, then $\varphi(r^n) = \varphi(r)^n = \bar{r}^n$. So
$$\bar{r}^n = 0 \pmod{\sqrt{0_R}} \iff \overline{r^n} \equiv 0 \pmod{\sqrt{0_R}} \iff r^n \in \sqrt{0_R} \iff r \in 0_R.$$

Exercise 4.6.7 (?)
Show that the nilradical is the intersection of all prime ideals.

Solution:

See A&M 1.8

Write P as the intersection of all prime ideals of R.
$\sqrt{0_R} \subseteq P$: Suppose $r \in \sqrt{0_R}$ so $r^n = 0$ and let $\mathfrak{p} \in \operatorname{Spec} R$. Then use that $0 \in I$ for any ideal: $r^n = 0 \in \mathfrak{p} \implies r \in \mathfrak{p}$ since $\mathfrak{p}$ is prime.
$\sqrt{0_R}^c \subseteq P^c$: Fix f non-nilpotent, we want to show f is not in any prime ideal. set $S \subseteq R$ to be all ideals I such that $f^{>0} \notin I$. Apply Zorn's lemma: $S \neq \emptyset$ since $0 \in S$, so after ordering I by inclusions S contains a maximal $\mathfrak{p}$ which we claim is prime. If $a, b \in \mathfrak{p}^c$ then $\mathfrak{p} + \langle a \rangle$ and $\mathfrak{p} + \langle b \rangle\, supset \mathfrak{p}$ strictly, and by maximality they aren't in S. So there exist m, n such that $f^m \in \mathfrak{p} + \langle a \rangle$ and $f^n \in \mathfrak{p} + \langle b \rangle$. Then $f^{m+n} \in \mathfrak{p} + \langle ab \rangle$, so $\mathfrak{p} + \langle ab \rangle$ is not in S. Thus $ab \notin \mathfrak{p}$ so $f \notin \mathfrak{p}$. Letting $\mathfrak{p}$ be arbitrary yields $f \notin P$.

Exercise 4.6.8 (?)
Show that $\sqrt{0_R} = \bigcap_{p \in \operatorname{Spec} R} p$ is the intersection of all prime ideals $p \trianglelefteq R$.

Definition 4.6.9 (Jacobson Radical)
The **Jacobson radical** $J(R)$ is the intersection of all maximal ideals, i.e.
$$J(R) = \bigcap_{\mathfrak{m} \in \operatorname{mSpec} R} \mathfrak{m}.$$

Exercise 4.6.10 (?)
Show $x \in J(R) \iff 1 - xR \subseteq R^\times$.

4.7 Structure Theorems

Definition 4.7.1 (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 4.7.2 (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.

Theorem 4.7.3 ***(Krull).***
Every ring has a proper maximal ideal, and any proper ideal is contained in a maximal ideal.

Theorem 4.7.4 ***(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 4.7.5.
If M is a simple ring over R a division ring, the M is isomorphic to a matrix ring.

Theorem 4.7.6 ***(Wedderburn).***
Every finite division ring is a field, i.e. finite division rings must be commutative.

4.8 Zorn's Lemma

Definition 4.8.1 (Chain in a poset)
In a poset, a **chain** is a totally ordered subset. An **upper bound** on a subset S of a poset X is any $x \in X$ such that $s \leq x$ for all $s \in S$.

Theorem 4.8.2 ***(Zorn's Lemma).***
If P is a poset in which every chain has an upper bound, then P has a maximal element.

Remark 4.8.3: You can always form a subset poset, and restrict with any sub-collection thereof with a set predicate. To use Zorn's lemma, you need to take an arbitrary chain in your poset X, produce an upper bound U (e.g. by taking a union), and showing that U is still in X (i.e. it still satisfies the right predicate).

Proposition 4.8.4 ***(Existence of maximal ideals).***
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.

■

Exercise 4.8.5 (?)
Show that every non-unit of R is contained in a maximal ideal.

Solution:
This follows because if $x \in R \setminus R^\times$, then $Rx \trianglelefteq R$ and $Rx \neq R$ implies $R/Rx \neq 0$. Then there exists some $\overline{\mathfrak{m}} \in \operatorname{mSpec} R/Rx$, and by the correspondence theorem this lifts to some $\mathfrak{m} \in \operatorname{mSpec} R$ containing Rx.

4.9 Unsorted

Fact 4.9.1
Division algorithm for Euclidean domains.

todo

Definition 4.9.2 (Field of fractions)
For $R \in \mathsf{CRing}$ an integral domain, the **field of fractions** of R can be constructed as

$$\mathrm{ff}(R) := (R \times R^{\bullet}) \,/\, \sim \qquad\qquad (a, s) \sim bt \iff at - bs = 0_R.$$

Checking transitivity requires having no nonzero zero divisors.

Definition 4.9.3 (Localization)
For $R \in \mathsf{CRing}$ and $S \subseteq R$ a *multiplicatively closed* subset, so $RS \subseteq S$ and $1_R \in S$, the **localization of** R **at** S can be constructed as

$$R\left[S^{-1}\right] := (R \times S) \,/\, \sim \qquad\qquad (a, s) \sim (b, t) \iff \exists u \in S \quad (at - bs)u = 0_R.$$

Why the u: use in proof of transitivity.

Universal property.

Warning 4.9.4
There is a canonical ring morphism

$$\begin{aligned} R &\to R\left[S^{-1}\right] \\ x &\mapsto \frac{x}{1}, \end{aligned}$$

but this may not be injective.

Remark 4.9.5: For integral domains R,

$$\mathrm{ff}(R) \cong R\left[(R^{\bullet})^{-1}\right].$$

Theorem 4.9.6 ***(Hilbert Basis Theorem).***

todo

Definition 4.9.7 (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.

Proposition 4.9.8 ***(Polynomial rings over UFDs are UFDs).***

todo

5 | Field Theory

Remark 5.0.1: Galois is defined as **normal and separable**.

Fact 5.0.2

- All fields are simple rings (no proper nontrivial ideals).
  - Thus every field morphism is either zero or injective.
- The characteristic of any field k is either 0 or p a prime.
- If L/k is algebraic, then $\min(\alpha, L)$ divides $\min(\alpha, k)$.

5.1 Basics: Polynomials

Definition 5.1.1 (Reducible and Irreducible Polynomials)
For $\mathbb{F}$ a field, a polynomial $f \in \mathbb{F}[x]$ is **reducible** if and only if f can be factored as $f(x) = g(x)h(x)$ for some $g, h \in \mathbb{F}[x]$ with $\deg g, \deg h \geq 1$ (so g, h are nonconstant). f is **irreducible** if f is not reducible.

Theorem 5.1.2 ***(Eisenstein's Criterion).***
If $f(x) = \displaystyle\sum_{i=0}^{n} \alpha_i x^i \in \mathbb{Q}[x]$ 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 $\mathbb{Z}[x]$.

Theorem 5.1.3 ***(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 5.1.4.
A primitive polynomial $p \in \mathbb{Q}[x]$ is irreducible $\iff p$ is irreducible in $\mathbb{Z}[x]$.

Definition 5.1.5 (Elementary Symmetric Functions)

todo

5.2 Definitions

Definition 5.2.1 (Characteristic)
The **characteristic** of a ring R is the smallest integer p such that $\sum_{k=1}^{p} 1 = 0$.

Proposition 5.2.2 ***(Freshman's Dream).***
If $\operatorname{ch} k = p$ then $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$.

Definition 5.2.3 (Fixed Field)
For $H \leq \underset{\mathsf{Fields}_k}{\operatorname{Aut}}(L)$,

$$L^H := \left\{ \ell \in L \;\middle|\; \sigma(l) = \ell \right\}.$$

Definition 5.2.4 (Prime Subfield)
The **prime subfield** of a field F is the subfield generated by 1.

Theorem 5.2.5 ***(Characterization of Prime Subfields).***
The prime subfield of any field is isomorphic to either $\mathbb{Q}$ or $\mathbb{F}_p$ for some p.

Definition 5.2.6 (Field Automorphisms)

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

Definition 5.2.7 (Embeddings and Lifts)
Let k denote a field, and L/k extension. Every field morphism is an embedding (injection). An *embedding* of k-algebras $L \hookrightarrow L'$ will refer to any ring morphism over k, i.e. a field morphism that restricts to the identity on k:

$$\begin{tikzcd}
L \arrow[rr, hook] & & L' \\
& k \arrow[ul, hook] \arrow[ur, hook] &
\end{tikzcd}$$

Link to Diagram

More generally, we can ask for lifts of any map $\sigma : k \to k_\sigma$:

$$\begin{tikzcd}
L \arrow[rr, hook] & {} & L' \\
k \arrow[u, hook] \arrow[rr, hook, "\sigma"] & {} \arrow[u, Rightarrow] & k_\sigma \arrow[u, hook]
\end{tikzcd}$$

Link to Diagram

Most often, we'll take $\sigma : k \to k$ to be the identity.

Definition 5.2.8 (Perfect Fields)
The following are equivalent:

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

Proposition 5.2.9 ***(Irreducible implies separable for perfect fields).***

todo

Definition 5.2.10 (Numerical Invariants)

- $$[L : K] = \dim_{\mathsf{Vect}_K} L,$$
  the dimension of L as a K-vector space
- $$\operatorname{Aut}(L/k) := \left\{ \sigma : L \to L' \;\middle|\; \sigma|_K = \mathrm{id}_K \right\},$$
  the lifts of the identity on K.
- $$\{L : K\} := \# \operatorname{Aut}(L/k) := \left\{ \sigma : L \to L' \;\middle|\; \sigma|_K = \mathrm{id}_K \right\},$$
  the number of lifts of the identity on K.
- $$\operatorname{Gal}(E/F) := \operatorname*{Aut}_{\mathsf{Fields}_k},$$
  if E is finite, normal, and separable.

Remark 5.2.11 ***(on general inequality):*** Note that in general,

$$|\operatorname{Aut}(L/k)| \leq [L : K],$$

with equality when L/k is Galois.

5.2.1 Extensions

Definition 5.2.12 (Simple Extensions)
An extension L/k is **simple** iff $L = K(\alpha)$ for some $\alpha \in L$.

Definition 5.2.13 (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 5.2.14 (Algebraic Extension)
A field extension L/k is **algebraic** iff every $\alpha \in L$ is the root of some polynomial $f \in k[x]$.

5.3 Extensions

Definition 5.3.1 (Distinguished Classes)
A collection of field extensions $\mathcal{S}$ is **distinguished** iff

1. For any tower $L/K/k$, the extension $L/k \in \mathcal{S} \iff L/K, K/k \in \mathcal{S}$, and
2. Lifts of distinguished extensions are distinguished: if $K/k \in \mathcal{S}$ and L/k is any extension, then $LK/k \in \mathcal{S}$:

$$\begin{tikzcd}
L & & L \\
K \arrow[u, hook] & \iff & K \arrow[u, hook] \arrow[u, hook, dashed, bend right] \\
k \arrow[u, hook] \arrow[uu, hook, dashed, bend right] & & k \arrow[u, hook] \arrow[u, hook, dashed, bend right]
\end{tikzcd}$$

Link to Diagram

$$\begin{tikzcd}
& LK & \\
L \arrow[ur, hook] & & K \arrow[ul, hook] \\
& k \arrow[ul, hook] \arrow[ur, hook] &
\end{tikzcd}$$

Link to Diagram

Note that if in addition $L/k \in \mathcal{S}$, then $LK/k \in \mathcal{S}$.

Supposed to think of LK/L as a lift of K/k.

Example 5.3.2 ***(of distinguished classes):***

- Algebraic extensions are distinguished.
- Finite extensions are distinguished.
- Separable extensions are distinguished.
- Normal extensions are *not* distinguished, but condition 2 holds: lifts of normal extensions are normal. Half of the forward implication of condition 1 holds: if L/k is normal, then L/K is normal.
  - Why: take $\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}(2^{\frac{1}{2}})/\mathbb{Q}$, each leg is normal since it's quadratic, but the overall extension misses complex roots. Similar issue for $\mathbb{Q}(2^{\frac{1}{3}}, \zeta_3)/\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}$, where now the bottom extension isn't normal.

5.3.1 Normal Extensions

Definition 5.3.3 (Normal Field Extension)
Let L/k be an extension. Then TFAE:

- L/k is **normal**.
- Every irreducible polynomial $f \in k[x]$ that has one root in L has *all* of its roots in L
  - So if $\alpha \in L$ then every Galois conjugate $\alpha_k \in L$ as well.. Thus either f splits in L or f has no roots in L.
- Every embedding $\sigma : L \hookrightarrow \bar{k}$ over k satisfies $\sigma(L) = L$, so σ is an automorphism of L over k.
- If L is separable and finite: L is the splitting field of some irreducible $f \in k[x]$.

Example 5.3.4 ***(of normal extensions):***

- If $[L : k] = 2$ then L/k is normal.
- $L := \mathbb{Q}(2^{\frac{1}{3}})$ is not normal, since $(x^3 - 2) = \prod_k x - \zeta_3^k 2^{\frac{1}{3}}$ with ζ_3, ζ_3^2 not in $L \subset \mathbb{R}$.
  - $L := \mathbb{Q}(2^{\frac{1}{4}})$ is not normal for the same reason.
- $\mathbb{Q}(\zeta_k)$ is normal for ζ_k any primitive kth root of unity.

Proposition 5.3.5 ***(?).***
For L/k finite, L is normal iff $L = \mathrm{SF}(f)$ is the splitting field for some $f \in k[x]$.

5.3.2 Separable Extensions

Definition 5.3.6 (Separable Field Extension)
Let L/k be a field extension, $\alpha \in L$ be algebraic over k, and $f(x) := \min(\alpha, k)$. The following are equivalent

- L/k is a **separable** extension.
- Every element $\alpha \in L$ is separable over k: α has separable minimal polynomial $\min_{\alpha,L}(x) \in \bar{k}[x]$ (D&F's definition, p. 551).
- f has no repeated factors/roots, i.e. f has no multiple roots in L.
- $\gcd(f, f') = 1$.
- $f' \not\equiv 0$
- Every finite subextension L'/k is separable.

If L/k is a finite extension, then, TFAE:

- L/k is separable.
- $L = k(\alpha)$ for α a separable element.
- $L = k(\{\alpha_i\})$ for α_i separable elements
- $[L : k] = \{L : k\} := \# \operatorname{Aut}_{\mathsf{Fields}_k}(L)$, the number of automorphisms over k.
- $[L : K] = [L : K]_s$, the separable degree.

Definition 5.3.7 (Separable degree)
Recall that a polynomial $p \in k[x]$ is **separable** if p has no multiple roots in $\bar{k}$ The **separable degree** of an extension L/k is defined by fixing an embedding $\sigma : k \hookrightarrow \bar{k}$ and letting $[L : k]_s$ be the number of lifts of σ to $\sigma' : L \to \bar{k}$:

$$\begin{tikzcd}
L \arrow[rr, hook, dashed] & & \bar{k} \\
& k \arrow[ul, hook] \arrow[ur, hook, "\sigma"'] &
\end{tikzcd}$$

Link to Diagram

Proposition 5.3.8 ***(Derivative criterion for separability).***
A polynomial f has multiple roots $\iff$ $\gcd(f, f') \neq 1$, and the multiple roots of f are precisely the roots of $\gcd(f, f')$.

Proof (?).
$\implies$ :: Write $f(x) := (x - a)^m g(x)$ with $m \geq 2$, then

$$f'(x) = m(x - a)^{m-1} g(x) + (x - a)^m g'(x)$$

and $(x - a)$ divides both factors.

$\not\Leftarrow$: If f has no multiple roots, $f(x) = \prod_i (x - a_i)$ and

$$f'(x) = \sum_j \prod_{i \neq j} (x - a_i).$$

Then fixing any a_k where $f(a_k) = 0$, check

$$f'(a_k) = \prod_{i \neq k} (x - a_i) \neq 0.$$

■

Proposition 5.3.9 ***(Separable splitting fields are Galois).***
If L/k is separable, then

$$[L:k] = \{L:k\}.$$

If L/k is a splitting field, then

$$[L:K] = \# \underset{\mathsf{Fields}_k}{\text{Aut}}(L) := \# \text{Gal}(L/k).$$

Proposition 5.3.10 ***(?).***
Irreducible polynomials have distinct roots after passing to a splitting field, i.e. irreducible polynomials have separable splitting fields.

5.3.3 Galois Extensions

Definition 5.3.11 (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. $\# \underset{\mathsf{Fields}_k}{\text{Aut}}(L) = [L:k] = \{L:k\}$ (D&F's definition).
3. The fixed field of $\text{Aut}(L/k)$ is exactly k.
4. L is the splitting field of a separable polynomial $p \in K[x]$.
5. L is finite, normal, and separable (most general definition?)

- L is a finite separable splitting field of an irreducible polynomial.
- L/k is separable and normal.
- The fixed field L^H for $H := \underset{\mathsf{Fields}_k}{\text{Aut}}(L)$ is precisely k.

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

$$\text{Gal}(L/k) := \underset{\mathsf{Fields}_k}{\text{Aut}}(L).$$

5.3.4 Special Extensions

Theorem 5.3.12 ***(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 5.3.13 ***(Primitive Element Theorem).***
Every finite separable extension is simple.

Corollary 5.3.14.
$\mathbb{GF}(p^n)$ is a simple extension over $\mathbb{F}_p$.

5.3.5 Quadratic Extensions

Proposition 5.3.15 ***(Classification of quadratic extensions).***
If $\mathbb{F}$ is a field with $\mathrm{ch}(\mathbb{F}) \neq 2$ and $E_{/\mathbb{F}}$ is a degree 2 extension, then E is Galois and $E = F(\sqrt{a})$ for some squarefree $a \in \mathbb{F}$.

Corollary 5.3.16 ***(Quadratic extensions of rationals).***
If $E_{/\mathbb{Q}}$ is a quadratic extension, $E = \mathbb{Q}(\sqrt{\frac{p}{q}})$ for some $p, q \in \mathbb{Z}$.

Proposition 5.3.17 ***(?).***
For $\mathbb{F}_p$ a finite field of prime order, all quadratic extensions $E/\mathbb{F}_p$ are isomorphic.

5.4 Finite Fields

Proof .
Todo

■

Proof

Theorem 5.4.1 *(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 5.4.2 *(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 5.4.3 *(Containment of Finite Fields).*
$\mathbb{GF}(p^\ell) \leq \mathbb{GF}(p^k) \iff \ell$ divides k.

Proposition 5.4.4 *(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 5.4.5 *(Splits Product of Irreducibles).*
Let $\rho_n := x^{p^n} - x$. Then $f(x) \mid \rho_n(x) \iff \deg f \mid n$ and f is irreducible.

Corollary 5.4.6.
$x^{p^n} - x = \prod f_i(x)$ 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 is squarefree and thus has no repeated factors. So φ_n is the product of all such irreducible f.

■

Proposition 5.4.7 ***(Finite fields are not algebraically closed).***
If $\mathbb{F}$ is a finite field then $F \neq \overline{F}$.

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

5.5 Cyclotomic Polynomials

Definition 5.5.1 (Cyclotomic Polynomials)
Let $\zeta_n = e^{2\pi i/n}$, then the n**th cyclotomic polynomial** is given by

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

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 $k < n$.
Note that $\deg \Phi_n(x) = \varphi(n)$ for φ the totient function.

Definition 5.5.2 (Cyclotomic Field)
Any subfield of $\mathrm{SF}(x^n - 1)$ is a **cyclotomic field**.

Proposition 5.5.3 ***(Computing Cyclotomic Polynomials).***
Computing Φ_n:

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

   where

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

2. $$x^n - 1 = \prod_{d \mid n} \Phi_d(x) \implies \Phi_n(x) = (x^n - 1)\left(\prod_{\substack{d \mid n \\ d<n}} \Phi_d(x)\right)^{-1},$$

so just use polynomial long division.

Fact 5.5.4 (computing cyclotomic polynomials, special cases and examples)

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

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

$$\begin{aligned}\Phi_1(z) &= z - 1 \\ \Phi_2(z) &= z + 1 \\ \Phi_4(z) &= z^2 + 1 \\ \Phi_6(z) &= z^2 - z + 1 \\ \Phi_8(z) &= z^4 + 1.\end{aligned}$$

Proposition 5.5.5 ***(Splitting Fields of Cyclotomic Polynomials).***
The splitting field of $x^m - 1$ is $\mathbb{Q}(\zeta_m)$ for ζ_m any primitive root of unity, and

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)_{/\mathbb{Q}}) \cong (\mathbb{Z}/m\mathbb{Z})^\times .$$

Theorem 5.5.6 ***(Kronecker-Weber).***
If $K_{/\mathbb{Q}}$ is an abelian extension, then $K \subseteq \mathbb{Q}(\zeta_m)$ for some m.

6 | Galois Theory

Proposition 6.0.1 ***(?).***
If $f \in k[x]$ is irreducible, then $\mathrm{Gal}(\mathrm{SF}(f)/k) \leq S_n$ is a transitive subgroup, i.e. it acts transitively on the set of roots.

Fact 6.0.2
Transitive subgroups of S_n for small n:

n in S_n	Transitive Subgroups
1	1
2	$\mathbb{Z}/2$
3	$S_3, \mathbb{Z}/3$
4	$S_4, A_4, D_4, (\mathbb{Z}/2)^2, \mathbb{Z}/4$

n in S_n	Transitive Subgroups
5	$S_5, A_5, F_5, D_5, \mathbb{Z}/5$

Proposition 6.0.3.
If $\operatorname{ch} k = 0$ or k is finite, then every *algebraic* extension L/k is separable.

Proposition 6.0.4.
If L/k is algebraic, then $\operatorname{Aut}(L/k)$ permutes the roots of irreducible polynomials.

Proposition 6.0.5.
$|\operatorname{Aut}(L/k)| \leq [L:k]$ with equality precisely when L/k is normal.

Theorem 6.0.6 ***(Dirichlet's Theorem on Arithmetic Progressions).***

todo

Definition 6.0.7 (Constructible)

todo

Theorem 6.0.8 ***(Constructibility of Regular n-gons).***

6.0.1 Lemmas About Towers

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

Proposition 6.0.9 ***(Towers are multiplicative in degree).***

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

Proposition 6.0.10 ***(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 6.0.11 ***(?).***
$\alpha \in L$ algebraic over $k \implies \alpha$ algebraic over F.

Corollary 6.0.12 ***(?).***

E_1/k normal and E_2/k normal $\implies$ E_1E_2/k normal and $E_1 \cap E_2/k$ normal.

$$\begin{tikzcd}
& E_1E_2 \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] \arrow[ddd, dashed, bend right, "\text{normal}"'] & \\
E_1 \arrow[dr, dash] \arrow[ddr, "\text{normal}"'] & & E_2 \arrow[dl, dash] \arrow[ddl, "\text{normal}"] \\
& E_1 \cap E_2 \arrow[d, dashed, "\text{normal}"] & \\
& k &
\end{tikzcd}$$

Link to diagram

Proposition 6.0.13 ***(Algebraicity is transitive).***

F/k algebraic and L/F algebraic $\implies$ L/k algebraic.

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

Proposition 6.0.14 ***(Separability is transitive).***

For $L/F/k$, then L/k is separable $\iff$ L/F, F/k are separable.

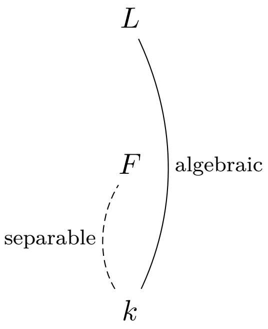
$$\begin{tikzcd}
L \arrow[d, bend right, "\text{sep}"'] \arrow[dd, dashed, bend left, "\text{sep}"] \\
F \arrow[d, bend right, "\text{sep}"'] \\
k
\end{tikzcd}$$

⚠ Warning 6.0.15

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

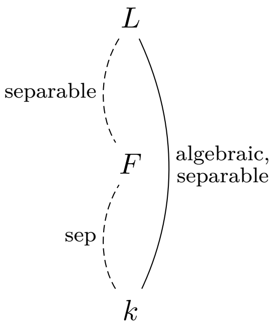
Proposition 6.0.16 ***(?).***

If L/k is algebraic, then F/k separable:



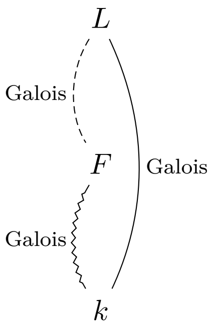
Link to diagram

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



Link to diagram

Proposition 6.0.17 ***(?).***
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,

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

6.0.2 Fundamental Theorem of Galois Theory

Theorem 6.0.18 ***(Fundamental Theorem of Galois Theory).***
Let L/k be a Galois extension, then there is a correspondence:

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

- 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 $\mathrm{Gal}(F/k) = \mathrm{Gal}(L/k)/H$.
- The compositum F_1F_2 corresponds to $H_1 \cap H_2$.
- The subfield $F_1 \cap F_2$ corresponds to H_1H_2.

6.0.3 Examples

Example 6.0.19 ***(Cyclotomic Fields):*** $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/(n)^\times$ and is generated by maps of the form $\zeta_n \mapsto \zeta_n^j$ where $(j, n) = 1$. I.e., the following map is an isomorphism:

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

Example 6.0.20 ***(Finite Fields):*** $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/\langle n\rangle$, a cyclic group generated by powers of the Frobenius automorphism:

$$\begin{aligned}\varphi_p : \mathbb{F}_{p^n} &\to \mathbb{F}_{p^n} \\ x &\mapsto x^p\end{aligned}$$

See D&F p.566 example 7.

Example 6.0.21 ***(Quadratic Fields):*** Every degree 2 extension L/k is Galois, except possibly in characteristic 2: if $\alpha \in L \setminus k$ then $\min_\alpha(x) \in L[x]$ must split in $L[x]$ since $\alpha \in L \implies \min_\alpha(x) = (x - \alpha)g(x)$ which forces $\deg(g) = 1$. So L is a splitting field. If $\mathrm{ch}(k) \neq 2$, then $\dfrac{\partial}{\partial x} \min_\alpha(x) = 2x - \cdots \not\equiv 0$, making L separable.

Proposition 6.0.22.
If K is the splitting field of an irreducible polynomial of degree n, then $\mathrm{Gal}(K/\mathbb{Q}) \leq S_n$ is a transitive subgroup.

Corollary 6.0.23.
n divides the order $|\mathrm{Gal}(K/\mathbb{Q})|$.

Theorem 6.0.24 ***(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 6.0.25 ***(Composite Extensions).***
If F/k is finite and Galois and L/k is arbitrary, then FL/L is Galois and

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

6.0.4 Counterexamples

Example 6.0.26 ***(?):***

- $\mathbb{Q}(\zeta_3, 2^{1/3})$ is normal but $\mathbb{Q}(2^{1/3})$ is not since the irreducible polynomial $x^3 - 2$ has only one root in it.
- $\mathbb{Q}(2^{1/3})$ is not Galois since its automorphism group is too small (only of size 1 instead of 3?).
- $\mathbb{Q}(2^{1/4})$ is not Galois since its automorphism group is too small (only of size 2 instead of 4). However, the intermediate extensions $\mathbb{Q}(2^{1/4})/\mathbb{Q}(2^{1/2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are Galois since they are quadratic. Slogan: "Being Galois is not transitive in towers."
- A quadratic extension that is not Galois: $\mathrm{SF}(x^2 + y) \in \mathbb{F}_2(y)[x]$, which factors as $(x - \sqrt{y})^2$, making the extension not separable.

7 Modules

Definition 7.0.1 (R-modules)
Four properties:

- $r(x+y) = rx + ry$
- $(r+s)x = rs + sx$
- $(rs)x = r(s(x))$
- $1_R x = x$

Proposition 7.0.2 ***(The one-step submodule test).***
$M \in \mathsf{R\text{-}Mod}$ iff for every $r \in R$ and $x, y \in M$, we have $rx + y \in M$.

7.1 General Theory

Definition 7.1.1 (Module Morphisms)
A map $f : M \to N$ is a **morphism of modules** iff $f(rm+n) = rf(m) + f(n)$.

Proposition 7.1.2 ***(Recognizing direct sums).***
If $M_1, M_2 \leq M$ are submodules, then $M = M_1 \oplus M_2$ if the following conditions hold:

- $M_1 + M_2 = M$
- $M_1 \cap M_2 = 0$

Definition 7.1.3 (Simple modules)
A module is **simple** iff it has no nontrivial proper submodules.

Definition 7.1.4 (Indecomposable modules)
A module M is **decomposable** iff it admits a direct sum decomposition $M \cong M_1 \oplus M_2$ with $M_1, M_2 \neq 0$. An **indecomposable** module is defined in the obvious way.

Definition 7.1.5 (Cyclic modules)
A module M is **cyclic** if there exists a single generator $m \in M$ such that $M = mR := \langle m \rangle$.

7.2 Free and Projective Modules

Definition 7.2.1 (Free Module)
A **free** module M is a module satisfying any of the following conditions:

- A universal property: There is a set $\mathcal{B}$ and a set map $M \xrightarrow{\iota} \mathcal{B}$ such that every set map $\mathcal{B} \xrightarrow{N}$ lifts:

$$\begin{tikzcd}
M \arrow[rd, dashed, "\tilde{f}"] & \\
\mathcal{B} \arrow[u, hook, "\iota"] \arrow[r, "f"] & N
\end{tikzcd}$$

Link to Diagram

- Existence of a basis:

  There is linearly independent (so $\sum r_i\beta_i = 0 \implies r_i = 0$) spanning set (so $m \in M \implies m = \sum r_i\beta_i$) of the form $\mathcal{B} := \{\beta_i\}_{i\in I}$,

- Direct sum decomposition:

  M decomposes as $M \cong \bigoplus_{i\in I} \beta_i R$, a sum of cyclic submodules.

Example 7.2.2 ***(A non-free module):*** $\mathbb{Z}/6$ is a $\mathbb{Z}$-module that is *not* free, since the element $[3]$ is a torsion element, where $2[3] = [6] = [0]$. This uses the fact that free modules over a PID are torsionfree.

Definition 7.2.3 (Free rank)
If a module M is free, the **free rank** of M is the cardinality of any basis.

Proposition 7.2.4 ***(?).***
Every free R-module admits a basis (spanning R-linearly independent set).

Definition 7.2.5 (Torsion and torsionfree)
An element $m \in M$ is a **torsion element** if there exists a nonzero $r \in R$ such that $rm = 0_M$. A module M is **torsion-free** if and only if for every $x \in M$, $mx = 0_M \implies m = 0_M$, i.e. M has no nonzero torsion elements. Equivalently, defining $M_t := \left\{ m \in M \;\middle|\; \exists r \in R, rm = 0_M \right\}$ as the set of all torsion elements, M is torsion free iff $M_t = 0$. If $M_t = M$, we say M is a **torsion module**.

Proposition 7.2.6 ***(Free implies torsionfree (generally)).***
For R an integral domain, any free R-module M is torsionfree.

Prove

Example 7.2.7 ***(A torsionfree module that is not free):*** $\mathbb{Q} \in \mathbb{Z}\text{-Mod}$ is torsionfree, but not free as a $\mathbb{Z}$-module. This follows because any two elements $a/b, p/q$ are in a single ideal, since taking $d := \gcd(b,q)$ we have $1/a = 1/d + \cdots 1/d$ and similarly $p/q = 1/a + \cdots + 1/a$, so these are in $\langle 1/d \rangle$. So any basis has size one, which would mean $\mathbb{Q} = \{\pm 1/d, \pm 2/d, \cdots\}$ which in particular doesn't include the average of the first two terms.

Definition 7.2.8 (Projective Modules)
A module P is **projective** iff it satisfies any of the following conditions:

- A universal property: for every surjective $N \xrightarrow{g} M$ and $P \xrightarrow{f} M$, the following lift exists:

$$\begin{tikzcd}
& P \arrow[d, "f"] \arrow[ld, dashed, "\exists \tilde{f}"'] & \\
N \arrow[r, two heads, "g"] & M \arrow[r] & 0
\end{tikzcd}$$

Link to Diagram

- Direct summand:

  P is a direct summand of a free module F, so $F = P \oplus T$ for some module $T \leq F$.

Proposition 7.2.9 ***(Free implies projective).***
Any free $M \in \mathsf{R\text{-}Mod}$ is projective.

Proof (?).

Todo: proof.

■

Example 7.2.10 ***(Projective $\not\Longrightarrow$ free):*** Let R_1, R_2 be two nontrivial rings and set $R := R_1 \oplus R_2$. Then R_1, R_2 are projective R-modules by construction, but each factor contains R-torsion: setting $e := (0, 1) \in R$ we have $e \curvearrowright R_1 = 0_{R_1}$. Since free implies torsionfree, R_1 can not be a free R-module.

7.3 Exact Sequences

Definition 7.3.1 (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 $\operatorname{im} d_i = \ker d_{i+1}$.

Definition 7.3.2 (Split Exact Sequences)
A short exact sequence

$$\xi : 0 \to A \xrightarrow{d_1} B \xrightarrow{d_2} C \to 0$$

has a **right-splitting** iff there exists a map $s : C \to B$ such that $d_2 \circ s = \mathbb{1}_C$. ξ has a **left-splitting** iff there exists a map $t : B \to A$ such that $t \circ d_1 = \mathbb{1}_A$.

Proposition 7.3.3 ***(Classifying split SESs).***
Let $\xi : 0 \to A \to B \to C \to 0$ be a SES, then TFAE

- ξ admits a right-splitting.
- ξ admits a left-splitting.
- ξ is isomorphic to a SES of the form $0 \to A \to A \oplus C \to C \to 0$.

Proposition 7.3.4 ***(Splitting Exact Sequences).***
A SES ξ splits if any of the following conditions hold:

- C is free.
- C is projective.
- A is injective.

7.4 Classification of Modules over a PID

Proposition 7.4.1 ***(STFGMPID).***
Let M be a finitely generated modules over a PID R. Then there is an **invariant factor** decomposition

$$M \cong F \bigoplus_{i=1}^{m} R/(r_i) \quad \text{where } r_1 \mid r_2 \mid \cdots$$

and similarly an **elementary divisor** decomposition:

$$M \cong F \bigoplus_{i=1}^{n} R/\left\langle p_i^{e_i} \right\rangle$$

where F is free of finite rank and the p_i are *not necessarily distinct* primes in R.

Proposition 7.4.2 ***(Principal Ideals are Free).***
If $I \trianglelefteq R$ is an ideal of R, then I 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.

■

7.5 Algebraic Properties

Definition 7.5.1 (Module structure on tensor products)

$$r \curvearrowright (m \otimes n) := (r \curvearrowright m) \otimes n.$$

Proposition 7.5.2 *(?).*
If $\dim_k V, \dim_k W < \infty$ then there is an isomorphism

$$\begin{aligned} V^\vee \otimes_k W &\xrightarrow{\sim} \underset{\mathsf{k\text{-}Mod}}{\operatorname{Hom}}(V, W) \\ \tilde{v} \otimes w &\mapsto \tilde{v}(-)w. \end{aligned}$$

Proposition 7.5.3 *(?).*
If either of $\dim_k V, \dim_k W$ is finite, then

$$\begin{aligned} V^\vee \otimes_k W^\vee &\xrightarrow{\sim} (V \otimes W)^\vee \\ v \otimes w &\mapsto (x \otimes y \mapsto v(x)w(y)). \end{aligned}$$

Proposition 7.5.4 *(?).*

$$\begin{aligned} \underset{\mathsf{k\text{-}Mod}}{\operatorname{Hom}}(V, W) &\xrightarrow{\sim} \underset{\mathsf{k\text{-}Mod}}{\operatorname{Hom}}(W, V)^\vee \\ T &\mapsto \operatorname{Tr}(T \circ -). \end{aligned}$$

Proposition 7.5.5 *(?).*
If $T : V \hookrightarrow W$ is injective, then $T \otimes \mathbb{1}_X : V \otimes X \hookrightarrow W \otimes X$ is also injective for any X. Thus $F(-) = (- \otimes X)$ is right-exact for any X.

Example 7.5.6 ***(Computing tensor products):*** $\mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}/3 = 0$:

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3 \arrow[r, "(-\times 2)\times \mathbb{1}"] \arrow[d, "\mathrm{proj}_2"] & \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3 \arrow[r] \arrow[d, "\mathrm{proj}_2"] & \mathbb{Z}/3 \otimes_{\mathbb{Z}} \mathbb{Z}/2 \arrow[d, dashed, "\cong"] \\
0 \arrow[r] & \mathbb{Z}/3 \arrow[r, "(-\times 2)"] & \mathbb{Z}/3 \arrow[r] & 0
\end{tikzcd}$$

Link to Diagram

8 Linear Algebra

8.1 Definitions

Remark 8.1.1: The main powerhouse: for $T : V \to V$ a linear transformation for $V \in \mathsf{Vect}_k$, map to $V \in \mathsf{k[x]\text{-}Mod}$ by letting polynomials act via $p(x) \cdot \mathbf{v} := p(T)(\mathbf{v})$. Using that $k[x]$ is a PID iff k is a field, and we can apply the FTFGMPID to get two decompositions:

$$V \cong \bigoplus_{i=1}^{n} k[x]/\left\langle q_i(x) \right\rangle \qquad\qquad q_i(x) \mid q_{i+1}(x) \mid \cdots$$

$$V \cong \bigoplus_{j=1}^{m} k[x]/\left\langle p_i(x)^{e_i} \right\rangle \qquad\qquad \text{with } p_i \text{ not necessarily distinct.}$$

- The q_i are the **invariant factors** of T
  - q_i is the minimal polynomial of T restricted to $V_i := k[x]/\left\langle q_i(x) \right\rangle$.
  - The largest invariant factor q_n is the **minimal polynomial** of T.
  - The product $\prod_{i=1}^{n} q_i(x)$ is the **characteristic polynomial** of T.
- The p_i are the **elementary divisors** of T.
  - Todo: what can you read off of this...?

Definition 8.1.2 (Nondegenerate Bilinear Form)

todo

Definition 8.1.3 (Quadratic Form)

todo

Definition 8.1.4 (Gram Matrix)

todo

Definition 8.1.5 (Normal Matrix)
A matrix $A \in \mathrm{Mat}(n \times n; \mathbb{C})$ is **normal** iff $A^*A = AA^*$ where A^* is the conjugate transpose.

Definition 8.1.6 (Semisimple)
A matrix A over k is **semisimple** iff A is diagonalizable over k^{Alg}, the algebraic closure.

Definition 8.1.7 (Nilpotent)
A matrix A over k is **nilpotent** iff $A^k = 0$ for some $k \geq 1$.

Idea: upper triangular matrices.

Definition 8.1.8 (Unipotent)
A element A in a ring R is **unipotent** iff $A - 1$ is nilpotent.

Idea: an upper-triangular matrix with ones on the diagonal.

Proposition 8.1.9 ***(Triangular Decomposition).***
Any linear map $T : V \to V$ over a perfect field decomposes as $T = S + N$ with S semisimple (diagonal), N nilpotent, and $[DN] = 0$. If T is invertible, then T decomposes as $T = SU$ where S is semisimple, U is unipotent, and $[UN] = 0$.

Proposition 8.1.10 ***(Perp of sum is intersection of perps).***

$$\left(\sum W_i\right)^{\perp} = \bigcap \left(W_i^{\perp}\right).$$

8.2 Minimal / Characteristic Polynomials

Remark 8.2.1: Fix some notation:

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

Definition 8.2.2 (?)
The **minimal polynomial** of a linear map T is the unique monic polynomial $\min_T(x)$ of minimal degree such that $\min_T(T) = 0$.

Definition 8.2.3 (?)
The **characteristic polynomial** of A is given by

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

Fact 8.2.4
If A is upper triangular, then $\det(A) = \prod_i a_{ii}$

Theorem 8.2.5 ***(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 8.2.6 (Similar Matrices)
Two matrices A, B are **similar** (i.e. $A = PBP^{-1}$) $\iff$ A, B have the same Jordan Canonical Form (JCF).

Definition 8.2.7 (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)

8.3 Finding Minimal Polynomials

Proposition 8.3.1 ***(How to find the minimal polynomial).***
Let $m(x)$ denote the minimal polynomial A.

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

this as $p(T) = 0$; then $\min_A(x) \mid p(x)$.

Definition 8.3.2 (Companion Matrix)
Given a monic $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} + x^n$, the **companion matrix** of p is given by

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

8.4 Canonical Forms

Proposition 8.4.1 ***(?).***
Let $T : V \to V$ be a linear map where $n := \dim_k V$. TFAE:

- There exists a basis $\{e_i\}$ of V such that

$$T(e_i) = \begin{cases} e_{i-1} & i \geq 2 \\ 0 & i = 1. \end{cases}$$

- There exists a cyclic vector $\mathbf{v}$ such that $\left\{ T^k \mathbf{v} \;\middle|\; k = 1, 2, \cdots, n \right\}$ form a basis for V.
- $T^{n-1} \neq 0$
- $\dim_k \ker T^\ell = \ell$ for each $1 \leq \ell \leq n$.
- $\dim_k \ker T = 1$.

8.4.1 Rational Canonical Form

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

Proposition 8.4.2 ***(Rational Canonical Form).***
$RCF(A)$ is a block matrix where each block is the companion matrix of an invariant factor of A.

Proof (Derivation of RCF).

- Let $k[x] \curvearrowright V$ by $p(x) \curvearrowright \mathbf{v} := p(T)(\mathbf{v})$, making V into a $k[x]$-module.

- k a field implies $k[x]$ a PID, so apply structure theorem to obtain an invariant factor decomposition
$$V \cong \bigoplus_{i=1}^{m} k[x]/\langle p_i(x)\rangle \qquad\qquad p_1(x) \mid p_2(x) \mid \cdots p_m(x).$$
- Each p_i is an invariant factor of T, and the minimal polynomial of T restricted to V_i.
- Write $V \cong \bigoplus_{i=1}^{m} V_i$ where $V_i := k[x]/\langle p_i(x)\rangle$, then A is a block matrix $\bigoplus_{i=1}^{m} M_i$ where M_i is the restriction of T to V_i:
$$\begin{pmatrix} M_1 & 0 & 0 & \cdots & 0 \\ 0 & M_2 & 0 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \cdots & & & M_n \end{pmatrix}.$$
- It suffices to determine the form of M_i, so without loss of generality suppose $m = 1$ so $V = V_1 = k[x]/\langle p(x)\rangle$ is a cyclic $k[x]$-module where $\deg p(x) = n$.
- Claim: the set $\{\mathbf{v}_i\}_{i=0}^{n-1} := \left\{\mathbf{v}, T\mathbf{v}, T^2\mathbf{v}, \cdots, T^{n-1}\mathbf{v}\right\}$ is a basis for V_1.
  - If there is any linear independence, this gives a polynomial relation $\sum_{i=1}^{n'} a_i T^i \mathbf{v} = 0$ for some $n' < n$, but then $q(x) := \sum_{i=1}^{n'} a_i x^i$ is a polynomial annihilating T, contradicting the minimality of $p(x)$.
  - So this yields n linearly independent vectors in k^n, so it's a basis.
- What is M_i in this basis? Check where basis elements are mapped to by T, noting that
$$p(T) = \sum_{i=1}^{n} a_i T^i \mathbf{v} = T^n + a_{n-1}T^{n-1}\mathbf{v} + a_{n-2}T^{n-2} + \cdots + a_1 T\mathbf{v} + a_0\mathbf{v} = 0,$$
we can write
  - $T\mathbf{v}_0 = \mathbf{v}_1$
  - $T\mathbf{v}_2 = T^2\mathbf{v}_0$
  - $T\mathbf{v}_3 = T^3\mathbf{v}_0$
  - $\cdots$
  - $T\mathbf{v}_{n-2} = T^{n-1}\mathbf{v}$
  - $T\mathbf{v}_{n-1} = T^n\mathbf{v} = -a_{n-1}T^{n-1}\mathbf{v} - \cdots - a_1 T\mathbf{v} - a_0\mathbf{v}$

  (using the minimal polynomial relation).
- So we have
$$M_1 = \begin{bmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & 0 & & -a_2 \\ & & \ddots & 0 & \vdots \\ & & & 1 & -a_{n-1} \end{bmatrix}.$$

■

8.4.2 Jordan Canonical Form

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

Lemma 8.4.3 ***(?).***
The elementary divisors of A are the minimal polynomials of the Jordan blocks.

Lemma 8.4.4 ***(JCF from Minimal and Characteristic Polynomials).***
Writing $\operatorname{Spec}(A) = \{(\lambda_i, b_i)\}$,

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

- 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

8.4.3 Smith Normal Form

Fact 8.4.5
For $A \in \operatorname{Mat}(m \times n; R)$ over R any PID, $\operatorname{SNF}(A)$ is a matrix whose diagonal entries are the invariant factors. How to compute $\operatorname{SNF}(A)$: take $A = \operatorname{diag}(a_i)$ where $a_i = d_i/d_{i-1}$ and d_i is the gcd of the determinants of all $i \times i$ minors of A. $A \sim B$ are similar $\iff \operatorname{SNF}(A) = \operatorname{SNF}(B)$.

8.4.4 Finding Possible Canonical Forms

Show how to find RCF and JCF from eigenvalues, or minimal/char polynomials.

8.4.5 Using Canonical Forms

Lemma 8.4.6 ***(?).***
The characteristic polynomial is the *product of the invariant factors*, i.e.

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

Lemma 8.4.7 ***(?).***
The minimal polynomial of A is the *invariant factor of highest degree*, i.e.

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

Proposition 8.4.8 ***(?).***
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

8.4.6 Computing Jordan Canonical Form

Proposition 8.4.9 ***(JCF Algorithm).***
The following algorithm always works for computing JCF(A):

- Compute $

8.5 Diagonalizability

Remark 8.5.1: *Notation:* A^* denotes the conjugate transpose of A.

Lemma 8.5.2*(?)*.
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 8.5.3*(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 8.5.4*(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 8.5.5 ***(Characterizations of Diagonalizability).***
M is diagonalizable over $\mathbb{F}$ $\iff$ $\underset{M}{\min}(x, \mathbb{F})$ splits into distinct linear factors over $\mathbb{F}$, or equivalently iff all of the roots of $\underset{M}{\min}$ lie in $\mathbb{F}$.

Proof (?).
$\implies$: If $\underset{A}{\min}$ 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.

■

8.6 Matrix Counterexamples

Example 8.6.1 ***(?):*** 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 $\mathbb{C}$
- $\underset{M}{\min}(x) = \chi_M(x) = x^2 + 1$

$$M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \sim \left(\begin{array}{r|r} -1\sqrt{-1} & 0 \\ \hline 0 & 1\sqrt{-1} \end{array}\right).$$

Example 8.6.2 ***(?):*** A matrix that:

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

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

Example 8.6.3 ***(?):*** Non-similar matrices with the same characteristic polynomial

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

Example 8.6.4 ***(?):*** A full-rank matrix that is not diagonalizable:

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

Example 8.6.5 ***(?):*** Matrix roots of unity, i.e. representations of i:

$$M_1 := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad M_2 := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

8.7 Matrix Groups

Definition 8.7.1 (General Linear Group)

$$\mathrm{GL}_n(\mathbb{R}) = \left\{ A \;\middle|\; A = \overline{A} \right\}.$$

Proposition 8.7.2 ***(Order of*** GL_n***).***

todo

Definition 8.7.3 (Special Linear Group)

$$\mathrm{SL}_n(\mathbb{C}) := \left\{ A \;\middle|\; \det A = 1 \right\}.$$

Definition 8.7.4 (Orthogonal Group)

$$O_n(\mathbb{C}) := \left\{ A \;\middle|\; A^t A = A A^t = I \right\}.$$

Dimension: $n(n-1)/2$.

Definition 8.7.5 (Special Orthogonal Group)

$$\mathrm{SO}_n(\mathbb{R}) = \left\{ A \;\middle|\; AA^t = I \right\} = \ker(\mathrm{GL}_n(\mathbb{R}) \to k^\times).$$

Definition 8.7.6 (Unitary Group)

$$U_n(\mathbb{C}) := \left\{ A \;\middle|\; A^\dagger A = A A^\dagger = 1 \right\}.$$

Definition 8.7.7 (Special Unitary Group)

$$\mathrm{SU}_n(\mathbb{C}) \coloneqq \left\{ A \in U_n(\mathbb{C}) \;\middle|\; \det A = 1 \right\}.$$

Definition 8.7.8 (Symplectic Group)

$$\mathrm{Sp}_{2n}(\mathbb{C}) \coloneqq \left\{ A \in \mathrm{GL}_{2n}(\mathbb{C}) \;\middle|\; A^t J A = J \right\} \qquad J \coloneqq \begin{bmatrix} 0 & 1_n \\ 1_n & 0 \end{bmatrix}.$$

Matrix group definitions.

9 Representation Theory

Theorem 9.0.1 ***(Schur's Lemma).***
If $M \in$ G-Mod is an irreducible representation of G with $\dim_k M < \infty$ and $k = \bar{k}$, then there is an isomorphism

$$M \xrightarrow{\sim} \operatorname*{Aut}_G(M, M).$$

Theorem 9.0.2 ***(Maschke's Theorem).***
Let k be a field with $\mathrm{ch}(k)$ not dividing $\#G$. Then any finite-dimensional representation of G decomposes into a direct sum of irreducible representations.

Definition 9.0.3 (Characters)
The **character** of a representation M is the trace of the map

$$\begin{aligned} T_g : M &\to M \\ m &\mapsto g \curvearrowright m. \end{aligned}$$

10 Extra Problems

10.1 Commutative Algebra

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

- Show that $\langle 2, x\rangle \trianglelefteq \mathbb{Z}[x]$ is not a principal ideal.

- Let R be a Noetherian ring and A, B algebras over R. Suppose A is finite type over R and finite over B. Then B is finite type over R.

10.2 Group Theory

10.2.1 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.

10.2.2 Primes in Group Theory

- Show that any group of prime order is cyclic and simple.

- Analyze groups of order pq with $q < p$.

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

  - Show that if q does not divide $p - 1$, then G is cyclic.
  - Show that G is never simple.

- Analyze groups of order p^2q.

Hint: Consider the cases when q does or does not divide $p^2 - 1$.

- Show that no group of order p^2q^2 is simple for $p < q$ primes.

- Show that a group of order p^2q^2 has a normal Sylow subgroup.

- Show that a group of order p^2q^2 where q does not divide $p^2 - 1$ and p does not divide $q^2 - 1$ is abelian.

- Show that every group of order pqr with $p < q < r$ primes contains a normal Sylow subgroup.

  - Show that G is never simple.

- 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.

10.2.3 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.

10.2.4 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.

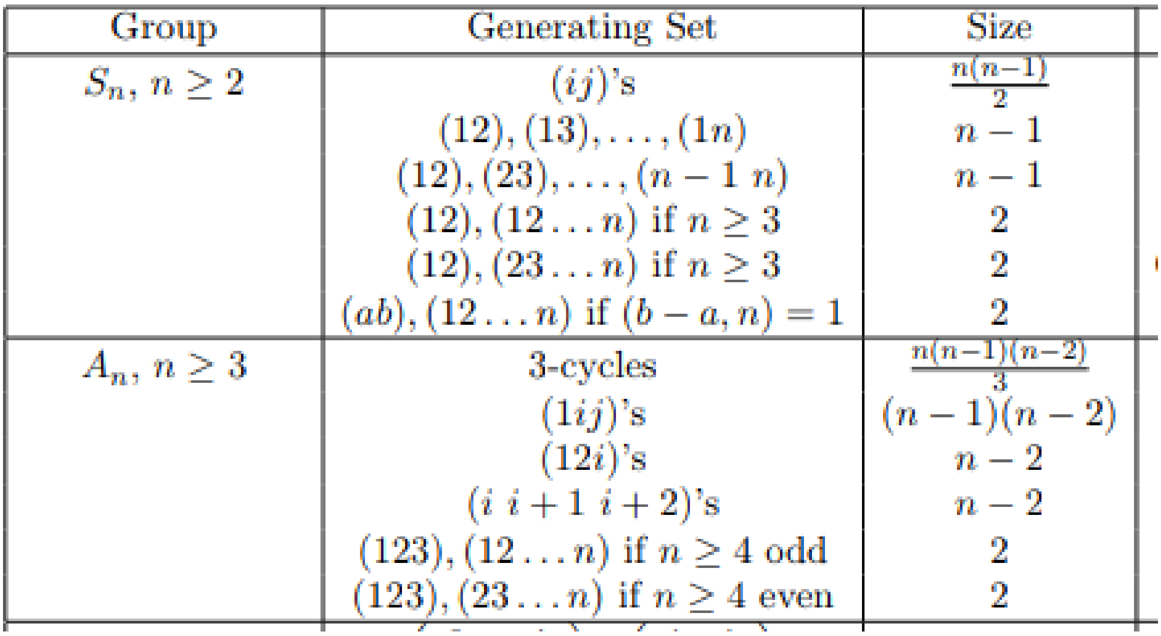
General Structure

- 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	$\frac{n(n-1)}{2}$
	$(12), (13), \dots, (1n)$	$n-1$
	$(12), (23), \dots, (n-1\ n)$	$n-1$
	$(12), (12 \dots n)$ if $n \geq 3$	2
	$(12), (23 \dots n)$ if $n \geq 3$	2
	$(ab), (12 \dots n)$ 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	$n-2$
	$(123), (12 \dots n)$ if $n \geq 4$ odd	2
	$(123), (23 \dots n)$ 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.

10.2.5 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.

10.2.6 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.

10.2.7 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.

10.2.8 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 products.

10.2.9 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.

10.2.10 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

10.2.11 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.

10.2.12 Nonstandard Topics

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

Thus "characteristic" is a strictly stronger condition than normality

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

So "characteristic" is a transitive relation for subgroups.

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

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

10.3 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 10.3.1 (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 10.3.2 (Maximal implies prime)
Maximal $\implies$ prime, but generally not the converse.

Solution:

- Suppose $\mathfrak{m}$ is maximal, $ab \in \mathfrak{m}$, and $b \not\in \mathfrak{m}$.
- 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 $\cup_{\mathfrak{m}\in\operatorname{maxSpec}(R)} = R \setminus R^{\times}$.
- Show that $\operatorname{maxSpec}(R) \subsetneq \operatorname{Spec}(R)$ 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 $\sqrt{0_(}R) = \sqrt{(0)}$.
- Show that $\operatorname{rad}(IJ) = \operatorname{rad}(I) \cap \operatorname{rad}(J)$
- Show that if $\operatorname{Spec}(R) \subseteq \operatorname{maxSpec}(R)$ 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 $\sqrt{(I)}$ is the intersection of all prime ideals containing I.

Problem 10.3.3 (Jacobson radical is bigger than the nilradical)
The nilradical is contained in the Jacobson radical, i.e.

$$\sqrt{\mathfrak{o}_(}R) \subseteq J\left(()R\right).$$

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

Problem 10.3.4 (Mod by nilradical to kill nilpotents)
$R/\sqrt{\mathfrak{o}_(}R)$ has no nonzero nilpotent elements.

Solution:

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

Problem 10.3.5 (Nilradical is intersection of primes)
The nilradical is the intersection of all prime ideals, i.e.

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

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

10.4 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 $ff(R[t]) = ff(R)(t)$.
- Show that $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$.
  - Show that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2} - \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- Show that the splitting field of $f(x) = x^3 - 2$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta_2)$.

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.

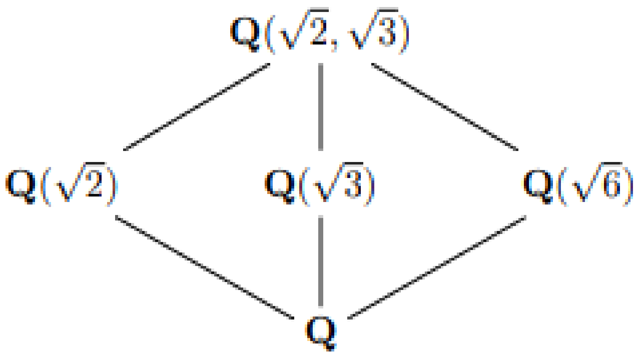
10.5 Galois Theory

10.5.1 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 $G(EF/k) \cong G(E/k) \times G(F/k)$.

10.5.2 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.

10.6 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.

10.7 Linear Algebra

Sort out from module section.

11 Even More Algebra Questions

Remark 11.0.1: (DZG): These all come from a random PDF I found, but I couldn't find the original author/source!

11.1 Groups

11.1.1 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?

11.1.2 Question 1.2

Prove that a subgroup of index two is normal.

11.1.3 Question 1.3

Find all normal subgroups of A_4.

11.1.4 Question 1.4

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

11.1.5 Question 1.5

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

11.1.6 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?

11.1.7 Question 1.7

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

11.1.8 Question 1.8

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

11.1.9 Question 1.9

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

11.1.10 Question 1.10

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

11.1.11 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 $p^r q^s$?

11.1.12 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.

11.1.13 Question 1.13

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

11.1.14 Question 1.14

Give examples of simple groups. Are there infinitely many?

11.1.15 Question 1.15

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

11.1.16 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.

11.1.17 Question 1.17

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

11.1.18 Question 1.18

Talk about conjugacy classes in the symmetric group S_n.

11.1.19 Question 1.19

When do conjugacy classes in S_n split in A_n?

11.1.20 Question 1.20

What is the centre of S_n? Prove it.

11.1.21 Question 1.21

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

11.1.22 Question 1.22

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

11.1.23 Question 1.23

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

11.1.24 Question 1.24

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

11.1.25 Question 1.25

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

11.1.26 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?

11.1.27 Question 1.27

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

11.1.28 Question 1.28

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

11.1.29 Question 1.29

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

11.1.30 Question 1.30

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

11.1.31 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?

11.1.32 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?

11.1.33 Question 1.33

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

11.1.34 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?

11.1.35 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?

11.1.36 Question 1.36

What groups have nontrivial automorphisms?

11.1.37 Question 1.37

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

11.1.38 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.

11.1.39 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.

11.1.40 Question 1.40

How many elements does $\mathfrak{gl}_2(\mathbb{F}_q)$ 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?

11.1.41 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.

11.1.42 Question 1.42

What are the subgroups of $\mathbb{Z}^2$?

11.1.43 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?

11.1.44 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?

11.2 Classification of Finite groups

11.2.1 Question 2.1

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

11.2.2 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 $\mathbb{Q}$?

11.2.3 Question 2.3

State/prove the Sylow theorems.

11.2.4 Question 2.4

Classify groups of order 35.

11.2.5 Question 2.5

Classify groups of order 21.

11.2.6 Question 2.6

Discuss groups of order 55.

11.2.7 Question 2.7

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

11.2.8 Question 2.8

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

11.2.9 Question 2.9

Classify all groups of order 8.

11.2.10 Question 2.10

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

11.2.11 Question 2.11

What are the groups of order p^2? What about pq? What if q is congruent to $1 \pmod p$?

11.2.12 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?

11.2.13 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?

11.2.14 Question 2.14

How many abelian groups are there of order 36?

11.2.15 Question 2.15

What are the abelian groups of order 16?

11.2.16 Question 2.16.

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

11.2.17 Question 2.17

How many abelian groups of order 200 are there?

11.2.18 Question 2.18

Prove there is no simple group of order 132.

11.2.19 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?

11.2.20 Question 2.20

Prove that there is no simple group of order 40.

11.3 Fields and Galois Theory

11.3.1 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.

11.3.2 Question 3.2

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

11.3.3 Question 3.3

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

11.3.4 Question 3.4

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

11.3.5 Question 3.5

What's the field with 25 elements?

11.3.6 Question 3.6

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

11.3.7 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.

11.3.8 Question 3.8

Are there separable polynomials of any degree over any field?

11.3.9 Question 3.9

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

11.3.10 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?

11.3.11 Question 3.11

What is a Galois extension?

11.3.12 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?

11.3.13 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.

11.3.14 Question 3.14

What is a Kummer extension?

11.3.15 Question 3.15

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

11.3.16 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?

11.3.17 Question 3.17

What is the discriminant of a polynomial?

11.3.18 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?

11.3.19 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.

11.3.20 Question 3.20

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

11.3.21 Question 3.21

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

11.3.22 Question 3.22

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

11.3.23 Question 3.23

What is the Galois group of

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \,/\, \mathbb{Q}?$$

11.3.24 Question 3.24

What is the Galois group of

$$\mathbb{Q}\left(\sqrt{n_1}, \cdots, \sqrt{n_m}\right) \,/\, \mathbb{Q}(\sqrt{n_1} + \cdots + \sqrt{n_m})?$$

11.3.25 Question 3.25

What are the Galois groups of irreducible cubics?

11.3.26 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?

11.3.27 Question 3.27

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

11.3.28 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?

11.3.29 Question 3.29

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

11.3.30 Question 3.30

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

11.3.31 Question 3.31

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

11.3.32 Question 3.32

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

11.3.33 Question 3.33

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

11.3.34 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.

11.3.35 Question 3.35

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

11.3.36 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?

11.3.37 Question 3.37

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

11.3.38 Question 3.38

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

11.3.39 Question 3.39

Describe the Galois theory of cyclotomic extensions.

11.3.40 Question 3.40

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

11.3.41 Question 3.41

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

11.3.42 Question 3.42

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

11.3.43 Question 3.43

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

11.3.44 Question 3.44

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

11.3.45 Question 3.45

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

11.3.46 Question 3.46

Give a polynomial with S_3 as its Galois group.

11.3.47 Question 3.47

Give an example of a cubic with Galois group S_3.

11.3.48 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.

11.3.49 Question 3.49

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

11.3.50 Question 3.50

Which finite groups are Galois groups for some field extension?

11.3.51 Question 3.51

What Galois group would you expect a cubic to have?

11.3.52 Question 3.52

Draw the subgroup lattice for S_3.

11.3.53 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?

11.3.54 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?

11.3.55 Question 3.55

How many automorphisms does the complex field have? How can you extend a simple automorphism $\sqrt{2} \mapsto -\sqrt{2}$ of an algebraic field into $\mathbb{C}$? How can you extend a subfield automorphism? What feature of $\mathbb{C}$ allows you to?

11.3.56 Question 3.56.

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

11.3.57 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 $1 \pmod{m}$.

11.3.58 Question 3.58

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

11.3.59 Question 3.59

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

11.3.60 Question 3.60

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

11.3.61 Question 3.61

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

11.3.62 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.

11.3.63 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?

11.3.64 Question 3.64

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

11.3.65 Question 3.65

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

11.3.66 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?

11.3.67 Question 3.67

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

11.3.68 Question 3.68

State and prove Eisenstein's Criterion.

11.3.69 Question 3.69

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

11.3.70 Question 3.70

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

11.3.71 Question 3.71

What are the symmetric polynomials?

11.3.72 Question 3.72

State the fundamental theorem of symmetric polynomials.

11.3.73 Question 3.73

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

11.3.74 Question 3.74

Find a non-symmetric polynomial whose square is symmetric.

11.3.75 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?

11.3.76 Question 3.76

Define p-adic numbers. What is a valuation?

11.3.77 Question 3.77

What's Hilbert's theorem 90?

11.3.78 Question 3.78

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

11.4 Normal Forms

11.4.1 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?

11.4.2 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.

11.4.3 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?

11.4.4 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?

11.4.5 Question 4.5

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

11.4.6 Question 4.6

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

11.4.7 Question 4.7

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

11.4.8 Question 4.8

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

11.4.9 Question 4.9

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

11.4.10 Question 4.10

What is rational canonical form?

11.4.11 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.

11.4.12 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.

11.4.13 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?

11.4.14 Question 4.14

What is a nilpotent matrix?

11.4.15 Question 4.15

When do the powers of a matrix tend to zero?

11.4.16 Question 4.16

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

11.4.17 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.

11.4.18 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 $SL_n(R)$?

11.4.19 Question 4.19

Is a square matrix always similar to its transpose?

11.4.20 Question 4.20

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

11.4.21 Question 4.21

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

11.5 Matrices and Linear Algebra

11.5.1 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?

11.5.2 Question 5.2

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

11.5.3 Question 5.3

Explain geometrically how you diagonalise a quadratic form.

11.5.4 Question 5.4

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

11.5.5 Question 5.5

Classify real division algebras.

11.5.6 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?

11.5.7 Question 5.7

Do you know about singular value decomposition?

11.5.8 Question 5.8

What are the eigenvalues of a symmetric matrix?

11.5.9 Question 5.9

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

11.5.10 Question 5.10

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

11.5.11 Question 5.11

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

11.5.12 Question 5.12

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

11.5.13 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.

11.5.14 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.

11.5.15 Question 5.15

State/prove the Cayley–Hamilton theorem.

11.5.16 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?

11.5.17 Question 5.17

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

11.5.18 Question 5.18

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

11.5.19 Question 5.19

What is a Toeplitz operator?

11.5.20 Question 5.20

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

11.6 Rings

11.6.1 Question 6.1

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

11.6.2 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?

11.6.3 Question 6.3

Is $\mathbb{C}[x, y]$ a PID? Is $\langle x, y\rangle$ a prime ideals in it?

11.6.4 Question 6.4

Do polynomials in several variables form a PID?

11.6.5 Question 6.5

Prove that the integers form a PID.

11.6.6 Question 6.6

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

11.6.7 Question 6.7

What is the relation between Euclidean domains and PIDs?

11.6.8 Question 6.8

Do you know a PID that's not Euclidean?

11.6.9 Question 6.9

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

11.6.10 Question 6.10

Is a ring of formal power series a UFD?

11.6.11 Question 6.11

Is a polynomial ring over a UFD again a UFD?

11.6.12 Question 6.12

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

11.6.13 Question 6.13

Give an example of a ring where unique factorisation fails.

11.6.14 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.

11.6.15 Question 6.15

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

11.6.16 Question 6.16

Find all primes in the ring of Gaussian integers.

11.6.17 Question 6.17

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

11.6.18 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?

11.6.19 Question 6.19

Do you know about Dedekind domains and class numbers?

11.6.20 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?

11.6.21 Question 6.21

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

11.6.22 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 $\sqrt{I}$.

11.6.23 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.

11.6.24 Question 6.24

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

11.6.25 Question 6.25

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

11.6.26 Question 6.26

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

11.6.27 Question 6.27

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

11.6.28 Question 6.28

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

11.6.29 Question 6.29

Is the following map an isomorphism?

$$\begin{aligned} \mathbb{Z}[t]/\left\langle t^p - 1 \right\rangle &\to \mathbb{Z}[w] \\ t &\mapsto w \text{ where } w^p = 1. \end{aligned}$$

11.6.30 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 $\underset{K}{\mathrm{End}}(V)$ 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.

11.6.31 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?

11.6.32 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?

11.6.33 Question 6.33

Define “Noetherian ring”. give an example.

11.6.34 Question 6.34

Prove the Hilbert basis theorem.

11.6.35 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?

11.6.36 Question 6.36

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

11.6.37 Question 6.37

Give an example of an Artinian ring.

11.6.38 Question 6.38

State the structure theorem for semisimple Artinian rings.

11.6.39 Question 6.39

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

11.6.40 Question 6.40

What is a matrix algebra?

11.6.41 Question 6.41

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

11.6.42 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?

11.6.43 Question 6.43

State the structure theorem for simple rings.

11.6.44 Question 6.44

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

11.6.45 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:

$$(f * g)(n) = \sum_{d \big| n} f(d) g\left(\frac{n}{d}\right).$$

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

11.6.46 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.

11.6.47 Question 6.47

Prove that all finite integral domains are fields.

11.6.48 Question 6.48

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

11.6.49 Question 6.49

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

11.6.50 Question 6.50

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

11.6.51 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 $\mathbb{Z}/5\mathbb{Z}$?

11.6.52 Question 6.52

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

11.7 Modules

11.7.1 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?

11.7.2 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?

11.7.3 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?

11.7.4 Question 7.4

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

11.7.5 Question 7.5

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

11.7.6 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?

11.7.7 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?

11.7.8 Question 7.8

What is a projective module?

11.7.9 Question 7.9

What is an injective module?

11.7.10 Question 7.10

Do you know an example of a flat module?

11.8 Representation Theory

11.8.1 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.

11.8.2 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?

11.8.3 Question 8.3

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

11.8.4 Question 8.4

State/prove/explain Schur’s lemma.

11.8.5 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?

11.8.6 Question 8.6

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

11.8.7 Question 8.7

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

11.8.8 Question 8.8

Why is the character table a square?

11.8.9 Question 8.9

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

11.8.10 Question 8.10

What's the regular representation?

11.8.11 Question 8.11

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

11.8.12 Question 8.12

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

11.8.13 Question 8.13

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

11.8.14 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?

11.8.15 Question 8.15

What is Frobenius reciprocity?

11.8.16 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?

11.8.17 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?

11.8.18 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?

11.8.19 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?

11.8.20 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.

11.8.21 Question 8.21

What are the irreducible representations of finite abelian groups?

11.8.22 Question 8.22

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

11.8.23 Question 8.23

Are there two nonisomorphic groups with the same representations?

11.8.24 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?

11.8.25 Question 8.25

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

11.8.26 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?

11.8.27 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?

11.8.28 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.

11.8.29 Question 8.29

Write the character table for S_4.

11.8.30 Question 8.30

Start constructing the character table for S_5.

11.8.31 Question 8.31.

How many irreducible representations does S_n have?

What classical function in mathematics does this number relate to?

11.8.32 Question 8.32

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

11.8.33 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?

11.8.34 Question 8.34

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

11.8.35 Question 8.35

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

11.8.36 Question 8.36

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

11.8.37 Question 8.37

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

11.9 Categories and Functors

11.9.1 Question 9.1

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

11.9.2 Question 9.2

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

11.9.3 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 $\mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})$?

12 | Appendix: Extra Topics

12.1 Characteristic Subgroups

Slogan 12.1.1
Normality is not transitive!

I.e. if $H \trianglelefteq G$ and $N \trianglelefteq H$, it's not necessarily the case that $N \trianglelefteq G$.

Definition 12.1.2 (Characteristic Subgroups)
A subgroup $H \leq G$ is **characteristic** in G, written $H \operatorname{ch} G$, iff for every $\varphi \in \operatorname{Aut}(G)$, $\varphi(H) \leq H$. Equivalently, $\varphi(H) = H$. I.e. H is fixed (not necessarily pointwise) under every automorphism of the ambient group G.

Remark 12.1.3*(Characteristic isn't equivalent to normalcy):* Characteristic subgroups are normal, because $\psi_g(-) \coloneqq g(-)g^{-1}$ is an (inner) automorphic of G. Not every normal subgroup is characteristic: take $G \coloneqq H_1 \times H_2$ and $\psi(x, y) = (y, x)$.

Proposition 12.1.4*(Fixing transitivity of normality).*
Characteristic subgroups of normal subgroups are normal, i.e. if $H \trianglelefteq G$ and $N \operatorname{ch} H$, then $N \trianglelefteq G$.

Proof (?).
$A \operatorname{ch} B \trianglelefteq C \implies A \trianglelefteq C$:

- $A \operatorname{ch} B$ iff A is fixed by every $\psi \in \operatorname{Aut}(B)$., WTS $cAc^{-1} = A$ for all $c \in C$.
- Since $B \trianglelefteq C$, the automorphism $\psi(-) \coloneqq c(-)c^{-1}$ descends to an element of $\operatorname{Aut}(B)$.
- Then $\psi(A) = A$ since $A \operatorname{ch} B$, so $cAc^{-1} = A$ and $A \trianglelefteq C$.

■

Proposition 12.1.5*(Centers are characteristic).*
For any group G,

$$Z(G) \operatorname{ch} G.$$

Proof (?).

Let $\psi \in \mathrm{Aut}(H)$ and $x = \psi(y) \in \psi(Z(H))$ so $y \in Z(H)$, then for arbitrary $h \in H$,

$$\begin{aligned}\psi(y)h &= \psi(y)(\psi \circ \psi^{-1})(h) \\ &= \psi(y \cdot \psi^{-1}(h)) \\ &= \psi(\psi^{-1}(h) \cdot y) && \text{since } \psi^{-1}(h) \in H,\, y \in Z(H) \\ &= h\psi(y).\end{aligned}$$

■

12.2 Normal Closures and Cores

Definition 12.2.1 (Normal Closure of a Subgroup)
The smallest normal subgroup of G containing H:

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

Definition 12.2.2 (Normal Core of a subgroup)
The largest normal subgroup of G containing H:

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

where

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

Theorem 12.2.3 ***(Fratini's Argument).***
If $H \trianglelefteq G$ and $P \in \mathrm{Syl}_p(G)$, then $HN_G(P) = G$ and $[G : H]$ divides $|N_G(P)|$.

12.2.1 Exercises

Exercise 12.2.4 (?)
Show that $Z(G) \leq G$ is always characteristic.

Solution:
Let $\psi \in \mathrm{Aut}(G)$. For one containment, we can show $\psi(g) = h = h\psi(g)$ for all $\psi(g) \in \psi(G)$

and $h \in G$. This is a computation:

$$\begin{aligned}\psi(g)h &= \psi(g)(\psi\psi^{-1})(h) \\ &= \psi(g)\psi(\psi^{-1}(h)) \\ &= \psi(\psi^{-1}(h)g) \\ &= (\psi\psi^{-1})(h)\psi(g) \\ &= h\psi(g).\end{aligned}$$

This yields $\psi(Z(G)) \subseteq Z(G)$. Applying the same argument to ψ^{-1} yields $\psi^{-1}(Z(G)) \subseteq Z(G)$. Since ψ is a bijection, $\psi\psi^{-1}(A) = A$ for all $A \leq G$, so $Z(G) \subseteq \psi(Z(G))$.

12.3 Nilpotent Groups

Definition 12.3.1 (Nilpotent)
A group G is **nilpotent** iff G has a terminating upper central series.

Moral: the adjoint map is nilpotent.

Theorem 12.3.2 ***(Characterization of Nilpotent Groups).***
G is nilpotent iff G has an upper central series terminating at G.

Theorem 12.3.3 ***(Characterization of Nilpotent Groups).***
G is nilpotent iff G has a lower central series terminating at 1.

Theorem 12.3.4 ***(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 12.3.5 ***(Nilpotent Implies Maximal Normals).***
A group G is nilpotent iff every maximal subgroup is normal.

Proposition 12.3.6.
For G a finite group, TFAE:

- G is nilpotent
- Normalizers grow, i.e. if $H < G$ is proper then $H < N_G(H)$.
- 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

Fact 12.3.7

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

Todo. Speci

13 UGA Fall 2019 Problem Sets

13.1 Problem Set One

13.1.1 Exercises

Problem 13.1.1 (Hungerford 1.6.3)
If $\sigma = (i_1 i_2 \cdots i_r) \in S_n$ and $\tau \in S_n$, then show that $\tau\sigma\tau^{-1} = (\tau(i_1)\tau(i_2)\cdots\tau(i_r))$.

Problem 13.1.2 (Hungerford 1.6.4)
Show that $S_n \cong \langle (12), (123\cdots n) \rangle$ and also that $S_n \cong \langle (12), (23\cdots n) \rangle$

Problem 13.1.3 (Hungerford 2.2.1)
Let G be a finite abelian group that is not cyclic. Show that G contains a subgroup isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$ for some prime p.

Problem 13.1.4 (Hungerford 2.2.12.b.)
Determine (up to isomorphism) all abelian groups of order 64; do the same for order 96.

Problem 13.1.5 (Hungerford 2.4.1)
Let G be a group and $A \trianglelefteq G$ be a normal abelian subgroup. Show that G/A acts on A by conjugation and construct a homomorphism $\varphi : G/A \to \mathrm{Aut}(A)$.

Problem 13.1.6 (Hungerford 2.4.9).)
Let $Z(G)$ be the center of G. Show that if $G/Z(G)$ is cyclic, then G is abelian.

Note that Hungerford uses the notation $C(G)$ for the center.

Problem 13.1.7 (Hungerford 2.5.6)
Let G be a finite group and$H \trianglelefteq G$ a normal subgroup of order p^k. Show that H is contained in every Sylow p-subgroup of G.

Problem 13.1.8 (Hungerford 2.5.9)
Let $|G| = p^n q$ for some primes $p > q$. Show that G contains a unique normal subgroup of index q.

13.1.2 Qual Problems

Problem 13.1.9
Let G be a finite group and p a prime number. Let X_p be the set of Sylow-p subgroups of G and n_p be the cardinality of X_p. Let $\mathrm{Sym}(X)$ be the permutation group on the set X_p.

1. Construct a homomorphism $\rho : G \to \mathrm{Sym}(X_p)$ with image a transitive subgroup (i.e. with a single orbit).
2. Deduce that if G is simple then the order of G divides $n_p!$.
3. Show that for any $1 \leq a \leq 4$ and any prime power p^k, no group of order ap^k is simple.

Solution:

1. Define the required group action by
$$\begin{aligned} \rho : G &\to \mathrm{Sym}(X_p) \\ g &\mapsto (\gamma_g : P \mapsto gPg^{-1}). \end{aligned}$$
The claim is that this action is transitive on X_p. This can be equivalently stated as
$$\forall P \in X_p, \exists g \in G, P' \in X_p \,\middle|\, gP'g^{-1} = P.$$
However, by Sylow 2, all Sylow $p-$subgroups are conjugate to each other, and thus this condition is satisfied.
2. Suppose that G is simple, so that we have
$$H \trianglelefteq G \implies H = \{e\} \text{ or } H = G.$$
Note that $\mathrm{Sym}(X_p) = (n_p)!$, and if we have an injective homomorphism $G \xrightarrow{\varphi} \mathrm{Sym}(X_p)$, then $|G| = |\varphi(G)|$, since $\varphi(G) \leq \mathrm{Sym}(X_p)$ will be a subgroup and thus have order dividing $(n_p)!$, which proves the statement.
Using the φ defined in (1), we can apply the first isomorphism theorem
$$G/\ker\varphi \cong \mathrm{im}\varphi \leq \mathrm{Sym}(X_p),$$
and so it suffices to show that $\ker\varphi = \{e\}$.
Note that since $\ker\varphi \trianglelefteq G$ and G is simple, we can only have $\ker\varphi = \{e\}$ or $\ker\varphi = G$.
Towards a contradiction, suppose $\ker\varphi = G$.
By definition, we have
$$\begin{aligned} \ker\varphi &= \{g \in G \,\middle|\, \gamma_g = \mathrm{id}_{X_p}\} \\ &= \{g \in G \,\middle|\, \forall P \in X_p,\ gPg^{-1} = P\} \\ &= \bigcap_{P \in X_p} N_G(P), \end{aligned}$$

and so the kernel of φ is the intersection of all of the normalizers of the Sylow $p-$subgroups.

But this means that $N_G(P) = G$ for every Sylow $p-$subgroup, which means that $n_p = 1$ and there is a unique P which must be normal in G. Since G is simple, this forces P to be trivial or the whole group.

Towards a contradiction, suppose $P = G$. Then G is a $p-$group and thus has order p^n. But then G has normal subgroups of order p^k for all $0 < k < n$, contradicting the simplicity of G.

But the only other option is that P is trivial, whereas we know nontrivial Sylow $p-$subgroups exist by Sylow 1.

Thus we can not have $\ker \varphi = G$, and so $\ker \varphi$ is trivial as desired.

3. Suppose $|G| = ap^k$, where $1 \leq a \leq 4$. Then by Sylow 3, we have $n_p = 1 \pmod{p}$ and n_p divides a. If $a = 1$, then $n_p = 1$, and so G can not be simple. Moreover, if $p \geq a$, then $n_p \leq a$ and $n_p = 1 \pmod{p}$ forces $n_p = 1$ again.

   So we can restrict our attention to $2 \leq a \leq 4$ and $p = 2, 3$, which reduces to checking the cases $ap^k = 2(3^k), 4(3^k)$, or $3(2^k)$ for $k \geq 1$.

   If $ap^k = 2(3^k)$, we have $n_3 = 1 \pmod{3}$ and $n_3 \mid 2$, which forces $n_3 = 1$, so this can not be a simple group.

   Similarly, if $ap^k = 4(3^k)$, then $n_3 = 1 \pmod{3}$ and n_3 divides 4, which forces $n_3 = 1$ and thus G can't be simple.

   If $ap^k = 3(2^k)$, then $n_2 = 1 \pmod{2}$ and n_2 divides 3, so $n_2 = 1, 3$. But then $n_3! = 6$, and if $k > 1$, we have $3(2^k) > 6 = n_3!$, so G can not be simple by the result in (2).

   If $k = 1$, then G is order 6, so G is isomorphic to either $\mathbb{Z}_6$ or S_3. The group S_3 is not simple, since $A_3 \trianglelefteq S_3$, and the only simple cyclic groups are of prime order, so $\mathbb{Z}_6$ is not simple. This exhausts all of the possible cases.

Problem 13.1.10
Let G be a finite group and let $N \trianglelefteq G$, and let p be a prime number and Q a subgroup of G such that $N \subset Q$ and Q/N is a Sylow $p-$subgroup of G/N.

1. Prove that Q contains a Sylow $p-$subgroup of G.

2. Prove that every Sylow $p-$subgroup of G/N is the image of a Sylow $p-$subgroup of G.

Solution:
Proof.

1. Since Q/N is a Sylow $p-$subgroup of G/N, we can write $|G/N| = p^k l$ where $\gcd(p, l) = 1$, and $|Q/N| = p^k$.

   We can then write $|G| = p^n m$ where $n \geq l$ and $l \,\Big|\, m$.

By the third isomorphism theorem, we have

$$\frac{G/N}{Q/N} \cong G/Q$$

and so

$$\left|\frac{G/N}{Q/N}\right| = \frac{|G/N|}{|Q/N|} = \frac{p^k l}{p^k} = l$$

and so $|G/Q| = l$ where $(p, l) = 1$, and thus

$$|G/Q| = |G|/|Q| = l \implies |G| = |Q|\, l.$$

We then have

$$p^n m = |Q|\, l,$$

and since $(p, l) = 1$, it must be the case that p^n divides $|Q|$. But since $Q \leq G$, this means that Q itself must be a Sylow $p-$ subgroup of G.

2. Let $P_N \in \operatorname{Syl}(p, G/N)$. By the subgroup correspondence theorem, $P_n = H/N$ for some $H \leq G$ such that $N \subseteq H$.

   So choose $P_H \in \operatorname{Syl}(p, H)$; the claim is that $P_H \in \operatorname{Syl}(p, G)$ and that $\dfrac{P_H N}{N} \cong P_N$, which exhibits P_N as the image of a Sylow $p-$subgroup of G.

   We first have $P_H \in \operatorname{Syl}(p, G)$, which follows because we have $[G/N, H/N] = [G : P_H]$ from the fourth isomorphism theorem, and thus $[G/N, P_N] = [G : P_H]$. In particular, since P_N is a Sylow $p-$subgroup, p does not divide $[G/N, P_N]$ and thus p doesn't divide $[G : P_H]$, which makes P_H a maximal $p-$subgroup in G and thus a Sylow $p-$subgroup.

   We then have $P_H N/N = P_N$, which follows because $P_H \leq H \implies P_H N/N \leq H/N = P_N \leq G/N$.

   However, it is also the case that $P_H N/N \in \operatorname{Syl}(p, G/N)$. This follows because

   1. $P_H N/N = P_H / P_H \cap N$ by the 2nd isomorphism theorem, so it is a $p-$group.
   2. $P_H \subseteq P_H N \subseteq G \implies p$ doesn't divide $[G : P_H N]$, since P_H is also a Sylow $p-$group of G and thus has maximal prime power dividing $|G|$.
   3. $N \subseteq P_H N \subseteq G \implies [G/N : P_H N/N] = [G : P_H N]$

   Taken together, this says that $P_H N/N$ is a p-group and p doesn't divide $[G/N, P_H N/N]$, so it is a maximal $p-$subgroup and $P_H N/N \in \operatorname{Syl}(p, G/N)$.

   But since $P_H N/N \leq P_N$ and $|P_H N/N| = |P_N|$, we must have $P_H N/N = P_N$ as desired.

□

Problem 13.1.11
Let G be a finite group and $H < G$ a subgroup. Let n_H be the number of subgroups of G that are conjugate to H. Show that n_H divides the order of G.

Solution:
.* Let

$$C_H = \{gHg^{-1} \mid g \in G\}$$

be the conjugacy class of H, so $|C_H| = n_H$.
We wish to show that n_H divides $|G|$.
Claim 1:

$$n_H = [G : N_G(H)],$$

where $N_G(H) \leq G$ is the normalizer of H in G.
Note that if this claim is true, then we can apply Lagrange's theorem, which states

$$A \leq G \implies |G| = [A : G] \; |A|,$$

which in this case translates to

$$|G| = [N_G(H) : G] \; |N_G(H)| = n_H \; |N_G(H)|.$$

Since n_H divides the right-hand side, it must divide the left-hand side as well, which is precisely what we would like to show.
Proof of Claim 1:
The normalizer of H in G, written $N_G(H)$, is the largest subgroup of G containing H such that $H \trianglelefteq N_G(H)$, i.e.

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

Now consider S, the set of left cosets of $N_G(H)$. Suppose there are k of them, so

$$[G : N_G(H)] = |S| \coloneqq k.$$

Then S can be written as

$$S = \{g_1 N_G(H), \; g_2 N_G(H), \; \cdots, \; g_k N_G(H)\}.$$

where each g_i is a distinct element of G yielding a distinct coset $g_i N_G(H)$. In particular, if $i \neq j$, then $g_i \neq g_j$, and $g_i N_G(H) \notin g_j N_G(H)$.
In particular, S acts on C_H,

$$S \curvearrowright C_H$$
$$g_i N_G(H) \curvearrowright H = g_i H g_i^{-1},$$

taking H to one of its conjugate subgroups.
So define

$$K \coloneqq \{g_i H g_i^{-1} \mid 1 \leq i \leq k\}.$$

Note that $K \subseteq C_H$, and has at most k elements.

We claim that K has k *distinct* elements, i.e. that each g_i takes H to a *distinct* conjugate subgroup. We have

$$\begin{aligned}
g_i H g_i^{-1} = g_j H g_j^{-1} \quad && \implies \\
g_j^{-1} g_i H g_i^{-1} g_j = H \quad && \implies \\
(g_j^{-1} g_i) H (g_j^{-1} g_i)^{-1} = H \quad && \implies \\
g_j^{-1} g_i \in N_G(H) \quad && \implies \\
g_i \in g_j N_G(H) \quad && \implies \\
g_i = g_j,
\end{aligned}$$

where the last line follows because we assumed that each coset contains at most one g_i. Thus K has k distinct elements, and so

$$= k = |K| \leq |C_H| = n_H.$$

We now claim that $k \geq n_H$ as well.
Let $H' \in C_H$ be any subgroup conjugate to H, so $H' = gHg^{-1}$ for some $g \in G$. Then $g = g_i$ for some i, so $g \in g_i N_G(H)$.
Thus $g = g_i n$ for some $n \in N_G(H)$, but $n \in N_G(H) \iff nHn^{-1} = H$ by definition, and so we have

$$\begin{aligned}
H' &= gHg^{-1} \\
&= (g_i n) H (g_i n)^{-1} \\
&= g_i (nHn^{-1}) g_i^{-1} \\
&= g_i H g_i^{-1} \in K.
\end{aligned}$$

Since $H' \in C_H$ was an arbitrary subgroup conjugate to H, this says that $C_H \subseteq K$ and thus

$$n_H = |C_H| \leq |K| = k$$

Thus

$$[G : N_G(H)] = k = |M| = |K| = n_H,$$

which is what we wanted to show. □

Problem 13.1.12
Let $G = S_5$, the symmetric group on 5 elements. Identify all conjugacy classes of elements in G, provide a representative from each class, and prove that this list is complete.

Solution:

Claim 1: Conjugacy classes in S_n are completely determined by cycle type.
This follows because of the result on homework 1, which says that for any two cycles $\tau, \sigma \in S_n$,

we have

$$\tau(s_1\ s_2\ \cdots\ s_k)\tau^{-1} = (\tau(s^1)\ \tau(s^2)\ \cdots\ \tau(s_k)).$$

In particular, this shows that the cycle type of a single cycle is invariant under conjugation. If an element $\sigma \in S_n$ is comprised of multiple cycles, say $\sigma = \sigma_1 \cdots \sigma_\ell$, then

$$\tau(\sigma)\tau^{-1} = \tau(\sigma_1 \cdots \sigma_\ell)\tau^{-1} = (\tau\sigma_1\tau^{-1}) \cdots (\tau\sigma_\ell\tau^{-1}),$$

which shows that the entire cycle type is preserved under conjugation. So each conjugacy class has exactly one cycle type, and distinct classes have distinct cycle types, so this completely determines the conjugacy classes.

Claim 2: Cycle types in S_n are in bijective correspondence with integer partitions of n.

This follows because any integer partition of n can be used to obtain a canonical representative of a conjugacy class of S_n: if $n = a_1 + a_2 + \cdots a_n$, we simply take a cycle of length a_1 the first a_1 integers in order, a cycle of length a_2 containing the integers $a_1 + 1$ to a_2 in order, and so on.

Conversely, any permutation can be written as a product of disjoint cycles, and when the cycles for fixed points are added in, every integer between 1 and n will appear, and the sum of the lengths of all cycles must sum to n. Thus taking the cycle lengths yields an integer partition of n.

All integer partitions of 5 are given below, along with a canonical representative of the associated conjugacy class.

$$\begin{array}{rr}
5 & (1\ 2\ 3\ 4\ 5) \\
4+1 & (1\ 2\ 3\ 4)(5) \\
3+2 & (1\ 2\ 3)(4\ 5) \\
3+1+1 & (1\ 2\ 3)(4)(5) \\
2+2+1 & (1\ 2)(3\ 4)(5) \\
2+1+1+1 & (1\ 2)(3)(4)(5) \\
1+1+1+1+1 & (1)(2)(3)(4)(5)
\end{array}$$

□

13.2 Problem Set Two

13.2.1 Exercises

Problem 13.2.1 (Hungerford 2.1.9)
Let G be a finitely generated abelian group in which no element (except 0) has finite order. Show that G is a free abelian group.

Problem 13.2.2 (Hungerford 2.1.10)

1. Show that the additive group of rationals $\mathbb{Q}$ is not finitely generated.
2. Show that $\mathbb{Q}$ is not free.
3. Conclude that Exercise 9 is false if the hypothesis "finitely generated" is omitted.

Problem 13.2.3 (Hungerford 2.5.8)
Show that if every Sylow $p-$subgroup of a finite group G is normal for every prime p, then G is the direct product of its Sylow subgroups.

Problem 13.2.4 (Hungerford 2.6.4)
What is the center of the quaternion group Q_8? Show that $Q_8/Z(Q_8)$ is abelian.

Problem 13.2.5 (Hungerford 2.6.9)
Classify up to isomorphism all groups of order 18. Do the same for orders 20 and 30.

Problem 13.2.6 (Hungerford 1.9.1)
Show that every non-identity element in a free group F has infinite order.

Problem 13.2.7 (Hungerford 1.9.3)
Let F be a free group and for a fixed integer n, let H_n be the subgroup generated by the set $\left\{x^n \;\middle|\; x \in F\right\}$. Show that $H_n \trianglelefteq F$.

13.2.2 Qual Problems

Problem 13.2.8
List all groups of order 14 up to isomorphism.

Problem 13.2.9
Let G be a group of order p^3 for some prime p. Show that either G is abelian, or $|Z(G)| = p$.

Problem 13.2.10
Let p, q be distinct primes, and let k denote the smallest positive integer such that p divides $q^k - 1$. Show that no group of order pq^k is simple.

Problem 13.2.11
Show that S_4 is a solvable, nonabelian group.

13.3 Problem Set Three

13.3.1 Exercises

Problem 13.3.1 (Hungerford 2.7.10)
Show that S_n is solvable for$n \leq 4$ but S_3 and S_4 are not nilpotent.

Problem 13.3.2 (Hungerford 2.8.3)
Show that if N is a simple normal subgroup of a group G and G/N has a composition series, then G has a composition series.

Problem 13.3.3 (Hungerford 2.8.9)
Show that any group of order p^2q(for primes p, q) is solvable.

Problem 13.3.4 (Hungerford 5.1.1)
Let F/K be a field extension. Show that

1. $[F : K] = 1$ iff $F = K$.
2. If $[F : K]$ is prime, then there are no intermediate fields between F and K.
3. If $u \in F$ has degree n over K, then n divides $[F : K]$.

Problem 13.3.5 (Hungerford 5.1.8)
Show that if $u \in F$ is algebraic of odd degree over K, then so is u^2, and moreover $K(u) = K(u^2)$.

Problem 13.3.6 (Hungerford 5.1.14)

1. If $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, compute $[F : \mathbb{Q}]$ and find a basis of $F/\mathbb{Q}$.
2. Do the same for $\mathbb{Q}(i, \sqrt{3}, \zeta_3)$ where ζ_3 is a complex third root of 1.

Problem 13.3.7 (Hungerford 5.1.16)
Show that in $\mathbb{C}$, the fields $\mathbb{Q}(i) \cong \mathbb{Q}(\sqrt{2})$ as vector spaces, but not as fields.

13.3.2 Qual Problems

Problem 13.3.8
Let R and S be commutative rings with multiplicative identity.

1. Prove that when R is a field, every non-zero ring homomorphism $\varphi : R \to S$ is injective.
2. Does (a) still hold if we only assume that R is a domain? If so, prove it, and if not

provide a counterexample.

Problem 13.3.9
Determine for which integers the ring $\mathbb{Z}/n\mathbb{Z}$ is a direct sum of fields. Carefully prove your answer.

Problem 13.3.10
Suppose that R is a commutative ring. Show that an element $r \in R$ is not invertible iff it is contained in a maximal ideal.

Problem 13.3.11

1. Give the definition that a group G must satisfy the be solvable.
2. Show that every group G of order 36 is solvable.

Hint: You may assume that S^4 is solvable.

13.4 Problem Set Four

13.4.1 Exercises

Problem 13.4.1 (Hungerford 5.3.7)
If F is algebraically closed and$E$ is the set of all elements in F that are algebraic over a field K, then E is an algebraic closure of K.

Problem 13.4.2 (Hungerford 5.3.8)
Show that no finite field is algebraically closed.
Hint: if $K = \{a_i\}_{i=0}^n$, consider

$$f(x) = a_1 + \prod_{i=0}^{n} (x - a_i) \in K[x]$$

where $a_1 \neq 0$.

Problem 13.4.3 (Hungerford 5.5.2)
Show that if $p \in \mathbb{Z}$ is prime, then $a^p = a$ for all $a \in \mathbb{Z}_p$, or equivalently $c^p \equiv c \pmod{p}$ for all $c \in \mathbb{Z}$.

Problem 13.4.4 (Hungerford 5.5.3)
Show that if $|K| = p^n$, then every element of K has a unique pth root in K.

Problem 13.4.5 (Hungerford 5.5.10)
Show that every element in a finite field can be written as the sum of two squares.

Problem 13.4.6 (Hungerford 5.6.1)
Let F/K be a field extension. Let $\mathrm{char} K = p \neq 0$ and let $n \geq 1$ be an integer such that $(p, n) = 1$. If $v \in F$ and $nv \in K$, then $v \in K$.

Problem 13.4.7 (Hungerford 5.6.8)
If $\mathrm{char} K = p \neq 0$ and $[F : K]$ is finite and not divisible by p, then F is separable over K.

13.4.2 Qual Problems

Problem 13.4.8
Suppose that α is a root in $\mathbb{C}$ of $P(x) = x^{17} - 2$. How many field homomorphisms are there from $\mathbb{Q}(\alpha)$ to:

1. $\mathbb{C}$,
2. $\mathbb{R}$,
3. $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$?

Problem 13.4.9
Let C/F be an algebraic field extension. Prove that the following are equivalent:

1. Every non-constant polynomial $f \in F[x]$ factors into linear factors over $C[x]$.
2. For every (not necessarily finite) algebraic extension E/F, there is a ring homomorphism $\alpha : E \to C$ such that $\alpha \Big|_F$ is the identity on F.

Hint: use Zorn's Lemma.

Problem 13.4.10
Let R be a commutative ring containing a field k, and suppose that $\dim_k R < \infty$. Let $\alpha \in R$.

1. Show that there exist $n \in \mathbb{N}$ and $\{c_0, c_1, \cdots c_{n-1}\} \subseteq k$ such that

$$a^n + c_{n-1}a^{n-1} + \cdots + c_1 a + c_0 = 0.$$

2. Suppose that (a) holds and show that if $c_0 \neq 0$ then a is a unit in R.
3. Suppose that (a) holds and show that if a is not a zero divisor in R, then a is invertible.

13.5 Problem Set Five

13.5.1 Exercises

Problem 13.5.1 (Hungerford 5.3.5)
Show that if $f \in K[x]$ has degree n and F is a splitting field of f over K, the $[F : K]$ divides $n!$.

Problem 13.5.2 (Hungerford 5.3.12)
Let E be an intermediate field extension in $K \leq E \leq F$.

1. Show that if $u \in F$ is separable over over K, then u is separable over E.
2. Show that if F is separable over K, then F is separable over E and E is separable over K.

Problem 13.5.3 (Hungerford 5.3.13)
Show that if $[F : K] < \infty$, then the following conditions are equivalent:

1. F is Galois over K
2. F is separable over K and F is a splitting field of some polynomial $f \in K[x]$.
3. F is a splitting field over K of some polynomial $f \in K[x]$ whose irreducible factors are separable.

Problem 13.5.4 (Hungerford 5.4.1)
Suppose that $f \in K[x]$ splits in$F$ as

$$f = \prod_{i=1}^{k} (x - u_i)^{n_i}$$

with the u_i distinct and each $n_i \geq 1$. Let

$$g(x) = \prod_{i=1}^{k} (x - u_i) = \sum_{i=1}^{k} v_i x^i$$

and let $E = K(\{v_i\}_{i=1}^{k})$. Then show that the following hold:

1. F is a splitting field of g over E.
2. F is Galois over E.
3. $\mathrm{Aut}_E(F) = \mathrm{Aut}_K(F)$.

Problem 13.5.5 (Hungerford 5.4.10 a/g/h)
Determine the Galois groups of the following polynomials over the corresponding fields:

1. $x^4 - 5$ over $\mathbb{Q}, \mathbb{Q}(\sqrt{5}), \mathbb{Q}(i\sqrt{5})$.
2. $x^3 - 2$ over $\mathbb{Q}$.
3. $(x^3 - 2)(x^2 - 5)$ over $\mathbb{Q}$.

Problem 13.5.6 (Hungerford 5.6.11)
If $f \in K[x]$ is irreducible of degree $m > 0$ and $\operatorname{char}(K)$ does not divide m, then f is separable.

13.5.2 Qual Problems

Problem 13.5.7
Let E/F be a Galois field extension, and let K/F be an intermediate field of E/F. Show that K is normal over F iff $\operatorname{Gal}(E/K) \trianglelefteq \operatorname{Gal}(E/F)$.

Problem 13.5.8
Let $F \subset L$ be fields such that L/F is a Galois field extension with Galois group equal to $D_8 = \left\langle \sigma, \tau \;\middle|\; \sigma^4 = \tau^2 = 1,\ \sigma\tau = \tau\sigma^3 \right\rangle$. Show that there are fields $F \subset E \subset K \subset L$ such that E/F and K/E are Galois field extensions, but K/F is not Galois.

Problem 13.5.9
Let $f(x) = x^3 - 7$.

1. Let K be the splitting field for f over $\mathbb{Q}$. Describe the Galois group of $K/\mathbb{Q}$ and the intermediate fields between $\mathbb{Q}$ and K. Which intermediate fields are not Galois over $\mathbb{Q}$?
2. Let L be the splitting field for f over $\mathbb{R}$. What is the Galois group $L/\mathbb{R}$?
3. Let M be the splitting field for f over $\mathbb{F}_{13}$, the field with 13 elements. What is the Galois group of $M/\mathbb{F}_{13}$?

13.6 Problem Set Six

13.6.1 Exercises

Problem 13.6.1 (Hungerford 5.4.11)
Determine all subgroups of the Galois group and all intermediate fields of the splitting (over $\mathbb{Q}$) of the polynomial $(x^3 - 2)(x^2 - 3) \in \mathbb{Q}[x]$.

Problem 13.6.2 (Hungerford 5.4.12)
Let K be a subfield of$\mathbb{R}$ and let $f \in K[x]$ be an irreducible quartic. If f has exactly 2 real roots, the Galois group of f is either S_4 or D_4.

Problem 13.6.3 (Hungerford 5.8.3)
Let φ be the Euler function.

1. $\varphi(n)$ is even for $n > 2$.

2. find all $n > 0$ such that $\varphi(n) = 2$.

Problem 13.6.4 (Hungerford 5.8.9)
If $n > 2$ and ζ is a primitive nth root of unity over $\mathbb{Q}$, then $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \varphi(n)/2$.

Problem 13.6.5 (Hungerford 5.9.1)
If F is a radical extension field of K and E is an intermediate field, then F is a radical extension of E.

Problem 13.6.6 (Hungerford 5.9.3)
Let K be a field, $f \in K[x]$ an irreducible polynomial of degree $n \geq 5$ and F a splitting field of f over K. Assume that $Aut_k(F) \simeq S_n$. Let u be a root of f in F. Then,

1. $K(u)$ is not Galois over K; $[K(u) : K] = n$ and $Aut_K(K(u)) = 1$ (and hence solvable).

2. Every normal closure over K that contains u also contains an isomorphic copy of F.

3. There is no radical extension field E of K such that $K \subset K(u) \subset E$.

13.6.2 Qual Problems

Problem 13.6.7

1. Let K be a field. State the main theorem of Galois theory for a finite field extension L/K

2. Let $\zeta_{43} := e^{2\pi i/43}$. Describe the group of all field automorphisms $\sigma : \mathbb{Q}(\zeta_{43}) \to \mathbb{Q}(\zeta_{43})$.

3. How many proper subfields are there in the field $\mathbb{Q}(\zeta_{43})$?

Problem 13.6.8
Let F be a field and let $f(x) \in F[x]$.

1. Define what is a splitting field of $f(x)$ over F.

2. Let F be a finite field with q elements. Let E/F be a finite extension of degree $n > 0$. Exhibit an explicit polynomial $g(x) \in F[x]$ such that E/F is a splitting of $g(x)$ over F. Fully justify your answer.

3. Show that the extension E/F in (2) is a Galois extension.

Problem 13.6.9
Let $K \subset L \subset M$ be a tower of finite degree field extensions. In each of the following parts, either prove the assertion or give a counterexample (with justification).

1. If M/K is Galois, then L/K is Galois

2. If M/K is Galois, then M/L is Galois.

13.7 Problem Set Seven

13.7.1 Exercises

Problem 13.7.1 (Hungerford 4.1.3)
Let I be a left ideal of a ring$R$, and let A be an $R-$module.

1. Show that if S is a nonempty subset of A, then

$$IS := \left\{ \sum_{i=1}^{n} r_i a_i \;\middle|\; n \in \mathbb{N}^*; r_i \in I; a_i \in S \right\}$$

is a submodule of A.

Note that if $S = \{a\}$, then $IS = Ia = \{ra \mid r \in I\}$.

2. If I is a two-sided ideal, then A/IA is an R/I module with the action of R/I given by

$$(r + I)(a + IA) = ra + IA.$$

Problem 13.7.2 (Hungerford 4.1.5)
If R has an identity, then a nonzero unitary R-module is **simple** if its only submodules are 0 and A.

1. Show that every simple $R-$module is cyclic.
2. If A is simple, every $R-$module endomorphism is either the zero map or an isomorphism.

Problem 13.7.3 (Hungerford 4.1.7)

1. Show that if A, B are R-modules, then the set $\operatorname{Hom}_R(A, B)$ is all R-module homomorphisms $A \to B$ is an abelian group with $f + g$ given on $a \in A$ by

   $$(f+g)(a) \coloneqq f(a) + g(a) \in B.$$

   Also show that the identity element is the zero map.
2. Show that $\operatorname{Hom}_R(A, A)$ is a ring with identity, where multiplication is given by composition of functions.

   Note that $\operatorname{Hom}_R(A, A)$ *is called the* ***endomorphism ring*** *of* A*.*
3. Show that A is a left $\operatorname{Hom}_R(A, A)$-module with an action defined by

   $$a \in A, f \in \operatorname{Hom}_R(A, A) \implies f \curvearrowright a \coloneqq f(a).$$

Problem 13.7.4 (Hungerford 4.1.12)
Let the following be a commutative diagram of R-modules and R-module homomorphisms with exact rows:
Prove the following:

1. If α_1 is an epimorphisms and α_2, α_4 are monomorphisms then α_3 is a monomorphism.
2. If α_5 is a monomorphism and α_2, α_4 are epimorphisms then α_3 is an epimorphism.

Problem 13.7.5 (Hungerford 4.2.4)
Let R be a principal ideal domain,A a unitary left R-module, and $p \in R$ a prime (and thus irreducible) element. Define

$$pA \coloneqq \{pa \mathrel{\Big|} a \in A\}$$
$$A[p] \coloneqq \{a \in A \mathrel{\Big|} pa = 0\}.$$

Show the following:

1. $R/(p)$ is a field.
2. pA and $A[p]$ are submodules of A.
3. A/pA is a vector space over $R/(p)$, with

   $$(r + (p))(a + pA) = ra + pA.$$

4. $A[p]$ is a vector space over $R/(p)$ with

$$(r+(p))a = ra.$$

Problem 13.7.6 (Hungerford 4.2.8)
If V is a finite dimensional vector space and

$$V^m := V \oplus V \oplus \cdots \oplus V \quad (m \text{ summands}),$$

then for each $m \geq 1$, V^m is finite dimensional and $\dim V^m = m(\dim V)$.

Problem 13.7.7 (Hungerford 4.2.9)
If F_1, F_2 are free modules of a ring with the invariant dimension property, then

$$\operatorname{rank}(F_1 \oplus F_2) = \operatorname{rank} F_1 + \operatorname{rank} F_2.$$

13.7.2 Qual Problems

Problem 13.7.8
Let F be a field and let $f(x) \in F[x]$.

1. State the definition of a splitting field of $f(x)$ over F.
2. Let F be a finite field with q elements. Let E/F be a finite extension of degree $n > 0$. Exhibit an explicit polynomial $g(x) \in F[x]$ such that E/F is a splitting field of g over F. Fully justify your answer.
3. Show that the extension in (b) is a Galois extension.

Problem 13.7.9
Let R be a commutative ring and let M be an R-module. Recall that for $\mu \in M$, the *annihilator* of μ is the set

$$\operatorname{Ann}(\mu) = \{r \in R \mid r\mu = 0\}.$$

Suppose that I is an ideal in R which is maximal with respect to the property there exists a nonzero element $\mu \in M$ such that $I = \operatorname{Ann}(\mu)$.
Prove that I is a *prime* ideal in R.

Problem 13.7.10
Suppose that R is a principal ideal domain and $I \trianglelefteq R$ is an ideal. If $a \in I$ is an irreducible element, show that $I = Ra$.

13.8 Problem Set Eight

13.8.1 Exercises

Problem 13.8.1 (Hungerford 4.4.1)
Show the following:

1. For any abelian group A and any positive integer m,
$$\mathrm{Hom}(\mathbb{Z}_m, A) \cong A[m] := \{a \in A \mid ma = 0\}.$$
2. $\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) \cong \mathbb{Z}_{\gcd(m,n)}$.
3. As a $\mathbb{Z}-$module, $\mathbb{Z}_m^* = 0$.
4. For each $k \geq 1$, $\mathbb{Z}_m$ is a $\mathbb{Z}_{mk}-$module, and as a $\mathbb{Z}_{mk}$ module, $\mathbb{Z}_m^* \cong \mathbb{Z}_m$.

Problem 13.8.2 (Hungerford 4.4.3)
Let$\pi : \mathbb{Z} \to \mathbb{Z}_2$ be the canonical epimorphism. Show that the induced map $\overline{\pi} : \mathrm{Hom}(\mathbb{Z}_2, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}_2, \mathbb{Z}_2)$ is the zero map. Conclude that $\overline{\pi}$ is not an epimorphism.

Problem 13.8.3 (Hungerford 4.4.5)
Let R be a unital ring, show that there is a ring homomorphism $\mathrm{Hom}_R(R, R) \to R^{op}$ where Hom_R denotes left $R-$module homomorphisms. Conclude that if R is commutative, then there is a ring isomorphism $\mathrm{Hom}_R(R, R) \cong R$.

Problem 13.8.4 (Hungerford 4.4.9)
Show that for any homomorphism$f : A \to B$ of left $R-$modules the following diagram is commutative:
where θ_A, θ_B are as in Theorem 4.12 and f^* is the map induced on $A^{**} := \mathrm{Hom}_R(\mathrm{Hom}(A, R), R)$ by the map
$$\overline{f} : \mathrm{Hom}(B, R) \to \mathrm{Hom}_R(A, R).$$

Problem 13.8.5 (Hungerford 4.6.2)
Show that every free module over a unital integral domain is torsion-free. Show that the converse is false.

Problem 13.8.6 (Hungerford 4.6.3)
Let A be a cyclic $R-$module of order $r \in R$.

1. Show that if s is relatively prime to r, then $sA = A$ and $A[s] = 0$.
2. If s divides r, so $sk = r$, then $sA \cong R/(k)$ and $A[s] \cong R/(s)$.

Problem 13.8.7 (Hungerford 4.6.6)
Let A, B be cyclic modules over $R$of nonzero orders r, s respectively, where r is *not* relatively prime to s. Show that the invariant factors of $A \oplus B$ are $\gcd(r, s)$ and $\operatorname{lcm}(r, s)$.

13.8.2 Qual Problems

Problem 13.8.8
Let R be a PID. Let $n > 0$ and $A \in M_n(R)$ be a square $n \times n$ matrix with coefficients in R. Consider the R-module $M := R^n/\operatorname{im}(A)$.

1. Give a necessary and sufficient condition for M to be a torsion module (i.e. every nonzero element is torsion). Justify your answer.
2. Let F be a field and now let $R := F[x]$. Give an example of an integer $n > 0$ and an $n \times n$ square matrix $A \in M_n(R)$ such that $M := R^n/\operatorname{im}(A)$ is isomorphic as an $R-$module to $R \times F$.

Problem 13.8.9

1. State the structure theorem for finitely generated modules over a PID.
2. Find the decomposition of the $\mathbb{Z}-$module M generated by w, x, y, z satisfying the relations

$$\begin{aligned} 3w + 12y + 3x + 6z &= 0 \\ 6y &= 0 \\ -3w - 3x + 6y &= 0. \end{aligned}$$

Problem 13.8.10
Let R be a commutative ring and M an $R-$module.

1. Define what a torsion element of M is .
2. Given an example of a ring R and a cyclic $R-$module M such that M is infinite and M contains a nontrivial torsion element m. Justify why m is torsion.
3. Show that if R is a domain, then the subset of elements of M that are torsion is an $R-$submodule of M. Clearly show where the hypothesis that R is a domain is used.

13.9 Problem Set Nine

13.9.1 Exercises

Problem 13.9.1 (Hungerford 7.1.3)

1. Show that the center of the ring $M_n(R)$ consists of matrices of the form rI_n where r is in the center of R.

   Hint: Every such matrix must commute with ϵ_{ij}, the matrix with 1_R in the i, j position and zeros elsewhere.

2. Show that $Z(M_n(R)) \cong Z(R)$.

Problem 13.9.2 (Hungerford 7.1.5)

1. Show that if A, B are (skew)-symmetric then $A + B$ is (skew)-symmetric.

2. Let R be commutative. Show that if A, B are symmetric, then AB is symmetric $\iff$ $AB = BA$. Also show that for any matrix $B \in M_n(R)$, both BB^t and $B + B^t$ are always symmetric, and $B - B^t$ is always skew-symmetric.

Problem 13.9.3 (Hungerford 7.1.7)
Show that similarity is an equivalence relation on $M_n(R)$, and *equivalence* is an equivalence relation on $M_{m \times n}(R)$.

Problem 13.9.4 (Hungerford 7.2.2)
Show that an $n \times m$ matrix Aover a division ring D has an $m \times n$ left inverse B (so $BA = I_m$) $\iff$ $\text{rank} A = m$. Similarly, show A has a right $m \times n$ inverse $\iff$ $\text{rank} A = n$.

Problem 13.9.5 (Hungerford 7.2.4)

1. Show that a system of linear equations

$$\begin{gathered} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m = b_1 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m = b_n \end{gathered}$$

   has a simultaneous solution $\iff$ the corresponding matrix equation $AX = B$ has a solution, where $A = (a_{ij}), X = [x_1, \cdots, x_m]^t$, and $B = [b_1, \cdots, b_n]^t$.

2. If A_1, B_1 are matrices obtained from A, B respectively by performing the same sequence of elementary **row** operations, then X is a solution of $AX = B$ $\iff$ X is a solution of $A_1X = B_1$.

3. Let C be the $n \times (m+1)$ matrix given by

$$C = \begin{pmatrix} a_{11} & \cdots & a_{1m} & b_1 \\ . & & & \\ a_{n1} & \cdots & a_{nm} & b_n \end{pmatrix}.$$

Then $AX = B$ has a solution $\iff$ rank$A$ = rank$C$ and the solution is unique $\iff$ rank$(A) = m$.

Hint: use part 2.

4. If $B = 0$, so the system $AX = B$ is homogeneous, then it has a nontrivial solution $\iff$ rank$A < m$ and in particular $n < m$.

Problem 13.9.6 (Hungerford 7.2.5)
Let R be a PID. For each positive integer r and sequence of nonzero ideals $I_1 \supset I_2 \supset \cdots \supset I_r$, choose a sequence $d_i \in R$ such that $(d_i) = I_i$ and $d_i \,\Big|\, d_{i+1}$.
For a given pair of positive integers n, m, let S be the set of all $n \times m$ matrices of the form $\begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix}$ where $r = 1, 2, \cdots, \min(m, n)$ and L_r is a diagonal $r \times r$ matrix with main diagonal d_i.
Show that S is a set of canonical forms under equivalence for the set of all $n \times m$ matrices over R.

13.9.2 Qual Problems

Problem 13.9.7
Let R be a commutative ring.

1. Say what it means for R to be a unique factorization domain (UFD).
2. Say what it means for R to be a principal ideal domain (PID)
3. Give an example of a UFD that is not a PID. Prove that it is not a PID.

Problem 13.9.8
Let A be an $n \times n$ matrix over a field F such that A is diagonalizable. Prove that the following are equivalent:

1. There is a vector $v \in F^n$ such that $v, Av, \cdots A^{n-1}v$ is a basis for F^n.
2. The eigenvalues of A are distinct.

Problem 13.9.9
Let $x, y \in \mathbb{C}$ and consider the matrix

$$M = \begin{bmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ y & 0 & 1 \end{bmatrix}$$

1. Show that $[0, 1, 0]^t$ is an eigenvector of M.
2. Compute the rank of M as a function of x and y.
3. Find all values of x and y for which M is diagonalizable.

13.10 Problem Set Ten

13.10.1 Exercises

Problem 13.10.1 (Hungerford 7.3.1)
Let B be an R-module. Show that if $r + r \neq 0$ for all $r \neq 0 \in R$, then an n-linear form $B^n \to R$ is alternating $\iff$ it is skew-symmetric.

Problem 13.10.2 (Hungerford 7.3.5)
If R is a field and $A, B \in M_n(R)$ are invertible then the matrix $A + rB$ is invertible for all but a finite number of $r \in R$.

Problem 13.10.3 (Hungerford 7.4.4)
Show that if q is the minimal polynomial of a linear transformation $\varphi : E \to E$ with $\dim_k E = n$ then $\deg q \leq n$.

Problem 13.10.4 (Hungerford 7.4.8).)
Show that $A \in M_n(K)$ is similar to a diagonal matrix $\iff$ the elementary divisors of A are all linear.

Problem 13.10.5 (Hungerford 7.4.10)
Find all possible rational canonical forms for a matrix $A \in M_n(\mathbb{Q})$ such that

1. A is 6×6 with minimal polynomial $q(x) = (x - 2)^2(x + 3)$.
2. A is 7×7 with $q(x) = (x^2 + 1)(x - 7)$.

Also find all such forms when $A \in M_n(\mathbb{C})$ instead, and find all possible Jordan Canonical Forms over $\mathbb{C}$.

Problem 13.10.6 (Hungerford 7.5.2)
Show that if φ is an endomorphism of a free k-module E of finite rank, then $p_\varphi(\varphi) = 0$.
Hint: If A is the matrix of φ and $B = xI_n - A$ then

$$B^a B = |B| I_n = p_\varphi I_n \in M_n(k[x]).$$

If E is a $k[x]$-module with structure induced by φ, and ψ is the $k[x]$-module endomorphism $E \to E$ with matrix given by B, then

$$\psi(u) = xu - \varphi(u) = \varphi(u) - \varphi(u) = 0 \qquad\qquad \forall u \in E.$$

Problem 13.10.7 (Hungerford 7.5.7)

1. Let φ, ψ be endomorphisms of a finite-dimensional vector space E such that $\varphi\psi = \psi\varphi$. Show that if E has a basis of eigenvectors of ψ, then it has a basis of eigenvectors for both ψ and φ simultaneously.

2. Interpret the previous part as a statement about matrices similar to a diagonal matrix.

13.10.2 Qual Problems

Problem 13.10.8
Let $M \in M_5(R)$ be a 5×5 square matrix with real coefficients defining a linear map $L : \mathbb{R}^5 \to \mathbb{R}^5$. Assume that when considered as an element of $M_5(\mathbb{C})$, then the scalars $0, 1+i, 1+2i$ are eigenvalues of M.

1. Show that the associated linear map L is neither injective nor surjective.

2. Compute the characteristic polynomial and minimal polynomial of M.

3. How many fixed points can L have?

   (That is, how many solutions are there to the equation $L(v) = v$ with $v \in \mathbb{R}^5$?)

Problem 13.10.9
Let n be a positive integer and let B denote the $n \times n$ matrix over $\mathbb{C}$ such that every entry is 1. Find the Jordan normal form of B.

Problem 13.10.10
Suppose that V is a 6-dimensional vector space and that T is a linear transformation on V such that $T^6 = 0$ and $T^5 \neq 0$.

1. Find a matrix for T in Jordan Canonical form.

2. Show that if S, T are linear transformations on a 6-dimensional vector space V which both satisfy $T^6 = S^6 = 0$ and $T^5, S^5 \neq 0$, then there exists a linear transformation A from V to itself such that $ATA^{-1} = S$.

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.