Algebra Qualifying Exam Review

Table of Contents

Contents

1 | Topics and Remarks 2

Remark 1.0.1: (DZG) on the structure of these notes: these are *extremely* disorganized at the moment, and only reflect some amalgamation of all of the random notes I made to myself while studying for qualifying exams. As a result, things are bound to be out of order, and likely useless pedagogically unless you've seen most of the material before. Moreover, this has been a long-running document (started in my undergrad years, so pre-2018), and since I've forgotten and rewritten certain things at various points, there may even be duplicated material (e.g. propositions stated/proved in multiple places, repeated exercises or statements, etc).

In any case, I'd love to hear if you do find it useful! Readers are welcome to email me with any questions, comments, errors/typos, suggestions for improvement, or just to say hello! 😄

Remark 1.0.2: Adapted from remark written by Roy Smith, August 2006:

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

1.1 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

Remark 2.0.1: Summary of useful qual tips:

- Slightly obvious but good to remember:
  - Subgroups of abelian groups are automatically normal.
  - If N is normal in G, then N is normal in any subgroup containing it.
  - If $N \leq G$ is the unique group of order $\#N$, then N is normal (since any conjugate must have the same size).
  - Using the subgroup correspondence: if $L/H \leq G/H$ then $L \leq G$ has size $\#(L/H)\#H$.
- Sizes and structure:
  - Quotienting by bigger groups yields smaller indices:

    $$1 \leq H \leq H \leq K \leq G \quad \text{apply}[G:-] \implies \#G = [G:1] \geq [G:H] \geq [G:K] \geq [G:G] = 1.$$

  - x is central iff $[x] = \{e\}$.

  - Unions aren't (generally) subgroups, intersections always are.
  - Coprime order subgroups intersect trivially.
  - Distinct subgroups of order p^n, p^m can intersect trivially *or* in subgroups of order p^ℓ.

- Conjugacy:
  - Sizes of conjugacy classes divide $\#G$ (by orbit-stabilizer).
  - Conjugate subgroups have equal cardinality.
  - Normal subgroups absorb conjugacy classes, and are thus unions of conjugacy classes.
  - Reasoning about conjugacy classes: in S_n they're precisely determined by cycle type, i.e. a partition of n.
  - Remembering the class equation: for literally any group action $\varphi : G \curvearrowright X$, one has $X = \text{Fix}(\varphi) \coprod' \text{Orb}(x_i)$ as a disjoint union of fixed points and nontrivial orbits, since orbits partition X. Then take your action to be $G \curvearrowright G$ by $\varphi : g.x \coloneqq gxg^{-1}$ to get $\text{Fix}(\varphi) = Z(G)$ and $\text{Orb}(x_i) = \left\{gx_ig^{-1}\right\} = [x_i]$ the conjugacy classes. Now apply orbit stabilizer to get $\text{Orb}(x) \cong G/\text{Stab}(x)$ where $\text{Stab}(x) = Z(x) = C_G(x)$ the centralizer.

- Cosets:
  - Cosets partition a group.
  - Anything dealing with indices $[G : H]$: try just listing the cosets.
  - $aH = bH \iff ab^{-1} \in H$.
  - Showing subgroup containment: $K \subseteq H$ iff $kH = H$ for all $k \in K$.

- Sylows:
  - If S_p is normal, then S_p is characteristic. This is useful if $H \leq G$ and $P \in \text{Syl}_p(H)$ is normal in H, then P is also normal in G.

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

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

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. It turns out that a group morphism between groups of the same size that is either injective or surjective is automatically a bijection, and the inverse is automatically a group morphism, so bijective group morphisms are isomorphisms.

Fact 2.2.2 (Bezout's Identity)
If $a, b \in \mathbb{Z}$ with $\gcd(a, b) = d$, then there exist $s, t \in \mathbb{Z}$ such that

$$as + bt = d.$$

This d can be computed using the extended Euclidean algorithm.

Remark 2.2.3: Useful context clue! In particular, this works when a, b are coprime and $d = 1$, since you can write $x^1 = x^{as+bt} = x^{as}x^{bt}$ to get interesting information about orders of elements. 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 (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 2.2.7: 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 surjective 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: $g \in H \iff g^{-1} \in H$.

Definition 2.3.2 (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.

Definition 2.3.3 (Commutator)
The **commutator subgroup** of G is denoted $[G, G] \leq G$. It is the subgroup *generated* by all

elementary commutators:

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

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, $H \subseteq [G,G]$.

Note that elements in $[G,G]$ are generally products *of elementary commutators, and not elementary themselves, since we're taking the group generated by them.*

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 (On subgroups)

- Show that the intersection of two subgroups is again a subgroup.
  - Hint: one-step subgroup test.
- Show that if $H \coloneqq C_m, K \coloneqq C_n \leq G$ are cyclic, then $H \cap K = C_d$ where $d \coloneqq \gcd(m,n)$.
- Show that the intersection of two subgroups with coprime orders is trivial.
- Show that the union of two subgroups H, K is a subgroup iff $H \subset K$, and so is generally *not* a subgroup.
- Show that subgroups with the *same* prime order are either equal or intersect trivially.
- **Important for Sylow theory**: show (perhaps by example) that if S_1, S_2 are distinct subgroups of order p^k, then it's possible for their intersection to be trivial **or** for them to intersect in a subgroup of order p^ℓ for $1 \leq \ell \leq k-1$.
- Give a counterexample where $H, K \leq G$ but HK is not a subgroup of G.

2.4 Conjugacy

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

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

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.

Useful qual fact: $[x] = \{x\} \iff x \in Z(G)$, 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 conjugate subgroups 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 $\psi \in \mathrm{Inn}(G)$, $\psi(N) = N$.

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 $Z(G)$.
Hint: use the class equation.

Solution:
Easy solution:

- Use that $\#H \bmod p = 1$ since $H \leq G$ and G is a p-group.
- Then use that H is a union of conjugacy classes, and since $e \in H$ there is at least one class of size 1, so

$$\#H = \#\coprod'[h_i] = \#[e] + \sum{}' \#[h_i]$$
$$\implies 0 \equiv \#H \equiv 1 + \sum{}' \#[h_i] \bmod p,$$

  and since each $\#[h_i]$ divides $\#H$, not all can be of size p^ℓ since then the sum would be $0 \bmod p$. So at least one other $\#[h_i] = 1$, making that h_i central.

Another solution:

- Idea: use the class equation to force p to divide $\#(H \cap Z(G))$. Applying it to H yields

$$H = Z(H) \coprod_{i=1}^{m} [h_i],$$

  where the $[h_i]$ are conjugacy classes of size greater than 1.
- Now use that $Z(H) = Z(G) \cap H$, and since p divides the LHS the result will follow if p divides the size of the disjoint union on the RHS.
- This is true because each $\#[h_i] \neq 1$ and $[h_i]$ divides $\#H$ which divides $\#G$ which is a power of p. So $p \mid \#[h_i]$ for each i.

2.5 Centralizing and Centers

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

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

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

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

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

Definition 2.5.2 (Normalizer)

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

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.

Definition 2.5.4 (Center)
The **center** of G is defined as

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

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

Exercise 2.5.5 (?)

- 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 normal subgroups are not necessarily contained in $Z(G)$.
  - Hint: consider the order 3 subgroup of S_3.

Solution:
The $G/Z(G)$ theorem:

- Write $H \coloneqq Z(G)$ and $G/H = \langle xH \rangle$ as a cyclic quotient.
- Fix $a, b \in G$, then $aH = x^n H$ and $bH = x^m H$.
- So $ax^{-n} = h_1, bx^{-m} = h_2$ where the h_i are now central.
- Now write $ab = (x^n h_1)(x^m h_2) = ba$ by commuting everything.

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 ***(Quotients by bigger subgroups yield smaller quotients).***
If $H \leq K \leq G$, then

$$\#G = [G : 1] \geq [G : H] \geq [G : K] \geq [G : G] = 1.$$

In particular, If $H, K \leq G$ are just arbitrary, since $H \cap K \leq H, K$ we have $[H : H \cap K] \geq [G : H]$ and $[G : K]$.

Proof (?).
Write $G/H \cap K \coloneqq G/J = \{h_1 J, \cdots, h_m J\}$ as distinct cosets where $m \coloneqq [G : H]$ and the h_i are all in H. Then $i \neq j \implies h_i h_j^{-1} \notin H \cap K$, but $h_i h_j^{-1} \in H$ since subgroups are closed under products and inverses, 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, so $[G : K] \geq m$.

■

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

Proof (?).

- $x \in xH$, since $e \in H$ because H is a subgroup and we can take $h = e$ to get $x = xe \coloneqq$

$xh \in xH$.

- The reverse containment is clear, so $G = \bigcup_{x \in G} xH$ 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

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

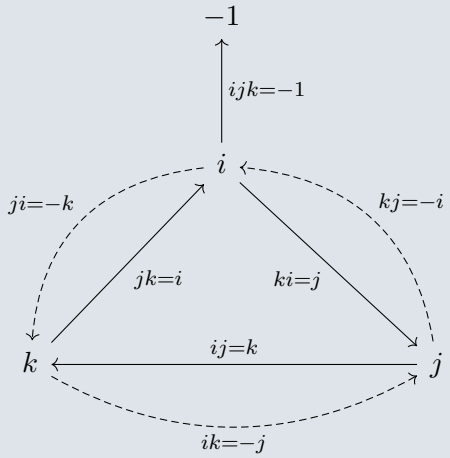
The r is a cycle of length n, and s is a reflection.
Examples of explicit cycle presentations:

- $D_4 = \langle (1,2,3,4), (1,3) \rangle$ which is a $2\pi/4$ rotation and a reflection through the diagonal line $y = -x$ in a square.
- $D_5 = \langle (1,2,3,4,5), (1,5)(2,4) \rangle$ which is a $2\pi/5$ rotation and a reflection about the line through vertex 3 in a pentagon.

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 $H \leq S_n$ is **transitive** iff its action on $\{1, 2, \cdots, n\}$ is transitive, i.e. for each pair (i, j) there is some element $\sigma \in H$ such that $\sigma(i) = j$. Note that σ may not fix other elements, and can have other effects!

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 $n \coloneqq \#G$ 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 $H_d \coloneqq \left\langle a^{\frac{n}{d}} \right\rangle$ 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:

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

Definition 2.7.8 (The sign homomorphism)

Writing a cycle as a product of transpositions, the map defined by

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

Remark 2.7.9:

- The kernel is the alternating group:
  - **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.
  - Examples: $(1,2,3)$ or $(1,2)(3,4)$ in S_4.
  - Non-examples: $(1,2)$ or $(1,2,3,4)$ in S_4, since they have an odd number of even length cycles.
- 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 usual integer parity of $k-1$.

Definition 2.7.10 (Alternating Group)
The **alternating group** is the subgroup of **even** permutations, i.e.

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

These are the permutations with an even number of even length cycles.

Proposition 2.7.11 ***(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 $(t_1 \dots t_{2k})$, 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 2.7.12 ***(Explicit alternating group):***

$$A_3 = \{\mathrm{id}, (1,2,3), (1,3,2)\},$$

which has cycle types $(1,1,1)$ and (3).

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

which has cycle types $(1,1,1,1), (2,2), (3,1)$.

A_5 is too big to write down, but has cycle types

- $(1,1,1,1,1)$
- $(2,2,1)$
- $(3,1,1)$
- (5)

Fact 2.7.13 (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 $p \not\equiv 1 \bmod q$ and $q \not\equiv 1 \bmod p$ 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 $N \coloneqq [G : H]$. 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

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

satisfying

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

Remark 2.10.2 ***(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
$\mathrm{Stab}(x) = G_x = \left\{ g \in G \;\middle|\; g \cdot x = x \right\} \leq G$	Stabilizer
$X/G \subseteq 2^X$	Set of Orbits
$\mathrm{Fix} = X^G = \left\{ x \in X \;\middle|\; g \cdot x = x \, \forall g \in G \right\} \subseteq X$	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, $x \in \text{Fix}$ iff $\text{Orb}(x) = \{x\}$ and $\text{Stab}_G(x) = G$.

Fact 2.10.3
For any group action, the kernel is the intersection of all stabilizers:

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

Definition 2.10.4 (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 2.10.5 ***(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 (of orbit stabilizer).

- 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 2.10.6 ***(Stabilizers of all orbit reps are conjugate).***
If $X \in G\text{-}\mathsf{Set}$, then for any points $x_i \in X$ in the same orbit, the stabilizers G_{x_0} and G_{x_1} are conjugate.
Note that if G acts transitively, this says all stabilizers are conjugate.

Proof (that stabilizers are conjugate).

- Fix $x \in X$ and $y \in \text{Orb}(x)$, so $g.x = y$ for some g.
- Let $H_x \coloneqq \text{Stab}(x)$ and $H_y \coloneqq \text{Stab}(y)$, the claim is that $H_x = g^{-1} H_y g$.

- Now just check:

$$\begin{aligned} h \in H_x &\iff hx = x \\ &\iff hg^{-1}y = g^{-1}y \\ &\iff ghg^{-1}y = y \\ &\iff ghg^{-1} \in H_y \\ &\iff h \in g^{-1}H_y g, \end{aligned}$$

so $H_x = g^{-1}H_y g$.

■

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

Remark 2.11.1 ***(The fixed-point count trick):*** A useful mnemonic: for any group action $\varphi : G \curvearrowright X$, using that orbits partition X we always have

$$X = \operatorname{Fix}(\varphi) \coprod_x{}' \operatorname{Orb}(x),$$

where $\operatorname{Fix}(\varphi)$ is the union of all orbits of size 1, and the remaining union is over distinct nontrivial orbits, taking one representative x from each.

Proposition 2.11.2 ***(Simple groups with a nontrivial subgroup embed into symmetric groups).***
An application of group actions: if G is simple, $H < G$ proper, and $[G : H] = n$, then there exists an injective map $\varphi : G \hookrightarrow S_n$.

Proof .

- Define a group action $\varphi : G \curvearrowright G/H \coloneqq \{eH, g_1H, \cdots, g_{n-1}H\}$ acting on the n cosets of H by left-translation $g.(g_kH) = (gg_k)H$.
- Then use that $\operatorname{Sym}(G/H) \leq S_n$, so $\operatorname{im}\varphi \leq S_n$ is a subgroup.
- Since G is simple and $\ker\varphi \leq G$, we have $\ker\varphi = 1, G$. If $\ker\varphi = 1$, φ is injective and we're done.

- Otherwise $\ker \varphi = G$, and acting on eH yields $gH = H$ for all g, forcing $H = G$ and $n = 1$, contradicting that $H < G$ is proper. ↯

■

2.11.1 Left Translation

Example 2.11.3 ***(The left translation action: trivial):*** Let G act on itself by left translation, where $\varphi : g \mapsto (h \mapsto gh)$.

- The orbit $\text{Orb}(x) = G$ is the entire group.
  - This action is transitive.
- The set of fixed points $\text{Fix}(\varphi) = \left\{ g \in G \;\middle|\; gx = x \,\forall x \in G \right\} = \{e\}$ is just the identity.
- The stabilizer $\text{Stab}(x) = \left\{ g \in G \;\middle|\; gx = x \right\} = \{e\}$ is just the identity.
- The kernel is the identity.
- Orbit stabilizer just says $G \cong G/\{e\}$.

2.11.2 Conjugation: The Class Equation and Burnside's Lemma

Example 2.11.4 ***(Conjugation yields centers/centralizers):*** Let G act on *itself* by conjugation, so $\varphi : g.x = gxg^{-1}$.

- The orbit $\text{Orb}(g) = [g]$ is the **conjugacy class** of g.
  - Thus the action is transitive iff G has only one single conjugacy class, which can only happen if $\#G = 1, 2$. On the other extreme, the orbits are all size 1 iff G is abelian.
- The set of fixed points $\text{Fix}(\varphi) = Z(G)$ is the **center**.
- The stabilizer is $\text{Stab}(g) = Z(g)$, the **centralizer** of g in G.
- The kernel is the intersection of all centralizers, i.e. again the **center** $Z(G)$.
- Orbit-stabilizer says $[g] = G/Z(g)$, so **the size of a conjugacy class is the index of the centralizer**.

Remark 2.11.5: Worth reiterating: $[G : Z(g)]$ is the number of elements in the conjugacy class $[g]$, and each $g \in Z(G)$ has a singleton conjugacy class $[g] = \{g\}$. Applying the fixed-point count

trick and substituting in orbit-stabilizer yields

$$\begin{aligned} G &= \mathrm{Fix}(\varphi) \coprod_x{}' \mathrm{Orb}(x) \\ &= Z(G) \coprod_g{}' [g] \\ &= Z(G) \coprod_g{}' \frac{G}{Z(g)}. \end{aligned}$$

Now taking cardinalities yields the class equation:

Corollary 2.11.6 ***(The Class Equation).***

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

As a reminder,

$$\begin{aligned} Z(g) &= \left\{ h \in G \;\middle|\; hgh^{-1} = g \right\} \text{ is the centralizer of } g \\ Z(G) &= \left\{ h \in G \;\middle|\; hgh^{-1} = g \ \forall g \in G \right\} = \bigcap_{g \in G} Z(g) \text{ is the center of } G. \end{aligned}$$

Exercise 2.11.7 (Applications of the class equation)

- Show that p groups have nontrivial centers.
- Show that groups of order p^2 are abelian.

Solution:
p-groups have nontrivial centers:

- Abusing notation by identifying sets with their cardinalities, the class equation says $G = Z(G) + \sum_g{}' [G : Z(g)]$ where the terms in the sum are all bigger than 1.
- Reducing mod p yields $0 = Z(g) + 0$, since p must divide $[G : Z(g)]$ when $[G : Z(g)] > 1$ because $G = [G : Z(g)]Z(g)$ and p divides the LHS.
- So p divides $Z(g)$, making $Z(g)$ nontrivial.

p^2 groups are abelian:

- $Z(G) = 1, p, p^2$, and by above we know $Z(G) \neq 1$. If $Z(G) = p^2$ we're done, so assume $Z(G) = p$.
- Then $G/Z(G) = p$ and groups of order p are cyclic, so the $G/Z(G)$ theorem applies and G is abelian.

Corollary 2.11.8 ***(Burnside's Lemma).***
For G a finite group acting on X,

$$\#X/G = \frac{1}{\#G}\sum_{g\in G} \#\mathrm{Fix}(g),$$

where $X/G = \{\mathrm{Orb}(x_1), \cdots, \mathrm{Orb}(x_n)\}$ is the set or orbits and $\mathrm{Fix}(g) = \left\{x \in X \;\middle|\; gx = x\right\}$ are the fixed points under g.

Slogan: the number of orbits is equal to the average number of fixed points.

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. Write $\mathrm{Stab}(x) = \left\{g \in G \;\middle|\; gx = x\right\}$ and $\mathrm{Fix}(g) = \left\{x \in X \;\middle|\; gx = x\right\}$.
First union over G, where the inner set lets x vary:

$$A = \coprod_{g_0\in G} \left\{(g_0, x) \;\middle|\; g_0 x = x\right\} \cong \coprod_{g_0\in G} \{g_0\} \times \mathrm{Fix}(g_0) \subseteq G \times X.$$

Then union over X, where the inner set lets g vary:

$$A = \coprod_{x_0\in X} \left\{(g, x_0) \;\middle|\; gx_0 = x_0\right\} \cong \coprod_{x_0\in X} \mathrm{Stab}(x_0) \times \{x_0\} \subseteq G \times X.$$

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

$$\sum_{g_0\in G} \#\mathrm{Fix}(g_0) = \#A = \sum_{x_0\in X} \#\mathrm{Stab}(x_0).$$

Now rearrange orbit-stabilizer:

$$\mathrm{Orb}(x_0) = G/\mathrm{Stab}(x_0) \implies \#\mathrm{Stab}(x_0) = \#G/\#\mathrm{Orb}(x_0),$$

and use this to rewrite the RHS:

$$\begin{aligned}
\sum_{g_0\in G} \#\mathrm{Fix}(g_0) &= \sum_{x_0\in X} \#\mathrm{Stab}(x_0) \\
&= \sum_{x_0\in X} \frac{\#G}{\#\mathrm{Orb}(x_0)} \\
&= \#G \sum_{x_0\in X} \frac{1}{\#\mathrm{Orb}(x_0)}
\end{aligned}$$

$$\implies \frac{1}{\#G}\sum_{g_0\in G} \#\mathrm{Fix}(g_0) = \sum_{x_0\in X} \frac{1}{\#\mathrm{Orb}(x_0)},$$

so it suffices to show the right-hand side sum is the number of orbits, $\#(X/G)$.

Proceed by partitioning the sum up according to which orbit each term comes from:

$$\begin{aligned}
\sum_{x_0 \in X} \left(\frac{1}{\#\mathrm{Orb}(x_0)} \right) &= \sum_{\mathrm{Orb}(x_0) \in X/G} \left(\sum_{y \in \mathrm{Orb}(x_0)} \left(\frac{1}{\#\mathrm{Orb}(x_0)} \right) \right) \\
&= \sum_{\mathrm{Orb}(x_0) \in X/G} \left(\frac{1}{\#\mathrm{Orb}(x_0)} \right) \sum_{y \in \mathrm{Orb}(x_0)} 1 \\
&= \sum_{\mathrm{Orb}(x_0) \in X/G} \left(\frac{1}{\#\mathrm{Orb}(x_0)} \right) \#\mathrm{Orb}(x_0) \\
&= \sum_{\mathrm{Orb}(x_0) \in X/G} 1 \\
&= \#(X/G).
\end{aligned}$$

■

2.11.3 Conjugation on Subgroups

Example 2.11.9 ***(?):*** Let G act on $X \coloneqq \left\{ H \;\middle|\; H \leq G \right\}$ (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 $\mathrm{Fix}(G)$ 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: $\ker \varphi = \bigcap_{H \leq G} N_G(H)$.
- Applying Orbit-stabilizer yields that the number of conjugates is the index of the normalizer:

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

2.11.4 Left Translation on Cosets

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

- The orbit $\mathcal{O}(xH) = G/H$, the entire set of cosets.

  - Note that this is a *transitive* action, since the trivial coset $eH \in G/H$ and its orbit is gH as g ranges over G, hitting every coset representative.

- The stabilizer $\text{Stab}(xH) = xHx^{-1}$, a **conjugate subgroup** of H.

  - This is because

$$\begin{aligned}
\text{Stab}(xH) &= \left\{g \in G \;\middle|\; gxH = xH\right\} \\
&= \left\{g \in G \;\middle|\; x^{-1}gx \in H\right\} \\
&= \left\{g \in G \;\middle|\; gx \in xH\right\} \\
&= \left\{g \in G \;\middle|\; g \in xHx^{-1}\right\} \\
&= xHx^{-1}.
\end{aligned}$$

- There are no fixed points, i.e. $\text{Fix}(G) = \emptyset$, since the action is transitive.
- The kernel of this action is $\ker\varphi = \bigcap_{g\in G} gHg^{-1}$, the intersection of all conjugates of H, sometimes called the **normal core** of H.

  - Note that if $\ker\varphi = G$ then H is normal, and if $\ker\varphi = 1$ then at least one conjugate doesn't intersect H nontrivially.

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 $\text{Sym}(X) \cong S_p$.
- Then $K := \ker\varphi$, and importantly $K \supseteq H$ since K is the intersection of stabilizers, and contains $\text{Stab}(eH) \supseteq H$ since $gH = H \implies g \in H$.
- Since G is finite and $K \leq G$, we have $\#(G/K)$ dividing $\#G$, since

$$[G : K] = \#(G/K) = \#G/\#K \implies \#G = \#(G/K)\#K.$$

- Now

$$G/K \cong K' \leq S_p \implies \#(G/K) \mid p!.$$

- So $\#(G/K)$ divides $\gcd(\#G, p!) = p$, using that p was the minimal prime dividing $\#G$. This forces $\#(G/K)$ to be 1 or p.
- If it's p:
  - Then $p = [G : K] = [G : H]$ and since $K \supseteq H$ this forces $K = H$. Kernels are automatically normal, so we're done.

- If it's 1:
  - Then $[G : K] = 1$ and $K = \ker \varphi = G$.
  - Identifying $\ker \varphi = \bigcap_{xH \in G/H} \mathrm{Stab}(xH)$, we have $\mathrm{Stab}(xH) = xHx^{-1} = G$ for all x, which says H is normal.

■

Exercise 2.11.12 (?)
Prove the Poincaré theorem for groups: if $H \leq G$ are possibly infinite groups with finite index $n \coloneqq [G : H]$, then there exists an $N \trianglelefteq H$ where $[N : H] < n!$.

3 Sylow Theorems

Remark 3.0.1: Useful facts:

- Counting contributions to $\#G$ from $\mathrm{Syl}_p(G)$: writing $\#G = p^k m$ so that $\#S_p = p^k$, using that every order p element is in some S_p one gets at least $n_p(\ell - 1)$ for some constant $\ell > 1$.
  - **Warning**: every S_p is the same size, so it's tempting to take $\ell \coloneqq \#S_p = p^k$. But this only works if one knows the S_p intersect trivially, e.g. if $k = 1$. Otherwise, the best one can do without more information $\ell = p$, i.e. the S_p all intersect trivially or in subgroups of order p.
  - **Warning**: This isn't quite a count of elements of order p, since elements in S_p can have orders $p^{k'}$ for other $k' \leq k$.
- When counting: just leave the identity out of every calculation, and add it back in as a $+1$ for the final count.

Definition 3.0.2
A **p-group** is a group G such that every element is order p^k for some k. If G is a finite p-group, then $|G| = p^j$ for some j.

Lemma 3.0.3 ***(Congruences for fixed points).***
If $G \curvearrowright X$ for G a p-group, then letting $\mathrm{Fix}(G) \coloneqq \left\{x \in X \;\middle|\; gx = x\right\}$, one has

$$\#X \equiv \#\mathrm{Fix}(G) \bmod p.$$

Proof (?).

- Use the fixed-point count trick:

$$\#X = \#\mathrm{Fix}(G) + \sum_x{}' \#\mathrm{Orb}(x).$$

Note that the result follows immediately by reducing $\bmod p$ if the sum is zero $\bmod p$.

- Letting x be an element with a nontrivial orbit, we have $\#\mathrm{Orb}(x) > 1$, so $\mathrm{Stab}(x) \neq G$ since orbit-stabilizer would yield $\#\mathrm{Orb}(x) = [G : \mathrm{Stab}(x)] = 1$.
- Now use that $\#\mathrm{Orb}(x) = \#G/\#\mathrm{Stab}(x) = p^k/p^\ell$ where $0 < \ell < k$ with strict inequalities. So $\#\mathrm{Orb}(x) = p^{k-\ell} \neq 1$, and p divides its size.

■

3.1 Statements of Sylow

For full proofs (some of which I've borrowed), see Keith Conrad's notes: https://kconrad.math.uconn.edu/blurbs/grouptheory/sylowpf.pdf

Remark 3.1.1: Some setup and notation: assume

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

3.1.1 Sylow 1 (Cauchy for Prime Powers)

Theorem 3.1.2 ***(Sylow 1).***

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

Slogan 3.1.3
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.

Proof (of Sylow 1: left translation).

- Let $\#G = p^k m$. Idea: Induct up by showing that if $\#H = p^i$ for $i \leq k$, one can product a bigger subgroup $\tilde{H} \supseteq H$ with $[\tilde{H} : H] = p$. This makes $\#\tilde{H} = p^{i+1}$.
- Let $H \leq G$ so that H is a p-group.
- Let $H \curvearrowright G/H$ by left-translation.
- Use the lemma that $\#(G/H) \equiv \mathrm{Fix}_H(G/H) \bmod p$
- Identify $\mathrm{Fix}_H(G/H) = N_G(H)$, since fixing xH means $gxH = xH \implies gHg^{-1} \subseteq$

$H \implies gHg^{-1} = H$ for all $g \in G$.

$$\begin{aligned} xH \in \mathrm{Fix}_H(G/H) &\iff gxH = xH \forall g \in H \\ &\iff x^{-1}gxH \in H \forall g \in H \\ &\iff x^{-1}Hx^{-1} = H \\ &\iff x \in N_G(H), \end{aligned}$$

so $\mathrm{Fix}_H(G/H) = \left\{ gH \;\middle|\; g \in N(H) \right\} = N_G(H)/H$ are cosets whose representatives are normalizers of H.

- Since $H \trianglelefteq N_G(H)$, these cosets form a group.
- We have $[G : H] = \#(N_G(H)/H)$, and if $i < k$ then p divides $[G : H]$.
- So $N_G(H)/H$ is a p-group and has a subgroup L of order p by Cauchy.
- Use the subgroup correspondence: $L \leq N_G(H)/H$ corresponds to some $L' \leq G$ with $H \subseteq L' \subseteq N_G(H)$ and $L = L'/H$. Now use that $\#L = p$ implies $\#(L'/H) = [L' : H] = p$, so $\#L' = [L' : H]\#H = p\#H = p^{i+1}$ as desired.

■

3.1.2 Sylow 2 (Sylows are Conjugate)

Theorem 3.1.4 ***(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 3.1.5.

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

Proof (of Sylow 2).

- Let $S_1, S_2 \in \mathrm{Syl}_p(G)$, and let $S_1 \curvearrowright G/S_2$ by left-translation.
- Use the lemma:

$$\#(G/S_2) \equiv \mathrm{Fix}_{S_1}(G/S_2) \bmod p.$$

- $[G : S_2] = m$ is coprime to p, so there is a fixed point, say xS_2 where $gxS_2 = xS_2$ for all $g \in S_1$.

$$\begin{aligned} &gxS_2 = xS_2 \forall g \in S_1 \\ \implies &gx \in xS_2 \forall g \in S_1 \\ \implies &S_1 x \subseteq xS_2 \\ \implies &S_1 \subseteq xS_2 x^{-1}, \end{aligned}$$

where we now get equality since these sets have the same cardinality.

■

3.1.3 Sylow 3 (Numerical Constraints)

Theorem 3.1.6 ***(Sylow 3).***

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

Proof (of Sylow 3).

- $n_p \equiv 1 \bmod p$:
  - Fix a $P \in \mathrm{Syl}_p(G)$, and let $P \curvearrowright \mathcal{S} \coloneqq \mathrm{Syl}_p(G)$ by conjugation.
  - Apply the lemma to get $n_p \equiv \mathrm{Fix}_{\mathcal{S}}(P) \bmod p$. The claim is that there is just one fixed point.
  - If $Q \in \mathrm{Fix}_{\mathcal{S}}(P)$, then $pQp^{-1} = Q$ for all $p \in P$, so P normalizes Q and $P \subseteq N_G(Q) \leq G$.
  - Then $P, Q \in \mathrm{Syl}_p(N_G(Q))$, which by Sylow II are conjugate.
  - Since $Q \trianglelefteq N_G(Q)$, there is only one conjugate of Q, and $P = Q$.
  - So P is the only fixed point.
- $n_p \mid m$:
  - Let $G \curvearrowright X \coloneqq \mathrm{Syl}_p(G)$ by conjugation; this is transitive by Sylow II and there is one orbit.
  - Then $\#X$ must divide $\$G$, so n_p divides $\#G = p^k m$.
  - Using $n_p \equiv 1 \bmod p$, we can't have $n_p \mid p^k$, and so n^p must divide m.
- $n_p = [G : N_G(P)]$ for any $P \in \mathrm{Syl}_p(G)$:
  - Let $G \curvearrowright \mathrm{Syl}_p(G)$ by conjugation and apply orbit-stabilizer to get $n_p = [G : \mathrm{Stab}(P)]$
  - Identify $\mathrm{Stab}(P) = N_G(P)$.

■

3.2 Corollaries and Applications

Corollary 3.2.1.
By Sylow 3, p does not divide n_p.

Proposition 3.2.2.
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 $H \coloneqq \cup_i H^i$ is maximal and thus a Sylow p-subgroup.

■

3.3 Exercises

Exercise 3.3.1 (?)

- 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.

3.4 Automorphism Groups

Fact 3.4.1

- 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 $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

- $\mathrm{Inn}(G) \cong G/Z(G)$.

3.5 Isomorphism Theorems

Theorem 3.5.1 ***(1st Isomorphism Theorem).***
If $\varphi : G \to H$ is a group morphism then

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

Note: for this to make sense, we also have

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

Corollary 3.5.2.
If $\varphi : G \to H$ is surjective then $H \cong G/\ker\varphi$.

Theorem 3.5.3 ***(Diamond Theorem / 2nd Isomorphism Theorem).***
If $S \leq G$ and $N \trianglelefteq G$, then

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

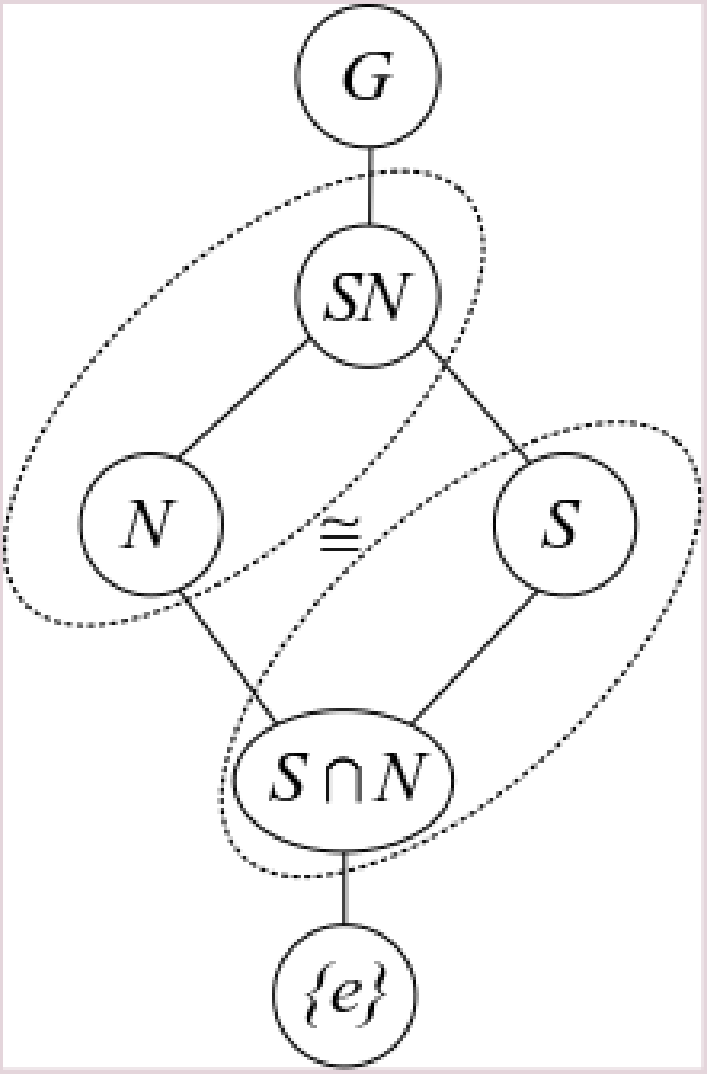


Figure 1: The 2nd "Diamond" Isomorphism Theorem

Remark 3.5.4: 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 3.5.5 ***(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 3.5.6 ***(The Correspondence Theorem / 4th Isomorphism Theorem).***
Suppose $N \trianglelefteq G$, then there exists a correspondence:

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

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 3.5.7
$N \trianglelefteq G$ and $N \subseteq H < G \implies N \trianglelefteq H$.

3.6 Products

Proposition 3.6.1 ***(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 3.6.2 ***(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 3.6.3 ***(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.

Exercise 3.6.4 (?)
Prove the "recognizing direct products" theorem. Can the conditions be relaxed?

Remark 3.6.5: Things are particularly nice when the orders of H and k are coprime. For 3, $x \in H \cap K$ implies that the order of x divides $\gcd(\#H, \#K) = 1$, so $H \cap K = \{e\}$. Thus for 2, one only needs that $\#(HK) = \#G$.

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):

$$\begin{aligned} \Gamma(h_1, k_1)\Gamma(h_2, k_2) &\coloneqq (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 \\ &= h_1(h_2k_1)k_2 \\ &= (h_1h_2)(k_1k_2) \\ &\coloneqq \Gamma((h_1, k_1)(h_2, k_2)). \end{aligned}$$

- 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 3.6.6 ***(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 3.6.7 ***(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.

3.7 Classification: Finitely Generated Abelian Groups

Definition 3.7.1 (Invariant Factor Decomposition)
If G is a finitely generated abelian group, then there is a decomposition

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

into a free group and a finite number of cyclic groups, where $r \in \mathbb{Z}^{\geq 0}$ is unique and the n_i are uniquely determined.

Definition 3.7.2 (Elementary Divisor Decomposition)
If G is a finitely generated abelian group, then there is a unique list of **not necessarily distinct** prime powers $p_k^{e_k}$ such that

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

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

Proposition 3.7.3 ***(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. Try it!

Example 3.7.4 ***(Abstract Example):***

Suppose G is given to you as a product of cyclic groups whose sizes factor in the following way

$$p_1^{e_1} p_1^{e_2} p_1^{e_3} \cdot p_2^{f_1} p_2^{f_2} \cdot p_3^{g_1} p_3^{g_2} p_3^{g_3} \cdot p_4^{h_1}.$$

Assemble these into a table, grouped by prime factor p_i, being careful not to separate primes from their exponents:

p_1	p_2	p_3	p_4
$p_1^{e_1}$		$p_3^{g_1}$	
$p_1^{e_2}$	$p_2^{f_1}$	$p_3^{g_2}$	
$p_1^{e_3}$	$p_2^{f_2}$	$p_3^{g_3}$	$p_4^{h_1}$

For elementary divisors: take columns, which just amounts to listing them again:

$$\begin{aligned}&\mathbb{Z}/p_1^{e_1} \times \mathbb{Z}/p_1^{e_2} \times \mathbb{Z}/p_1^{e_3} \\ &\times \mathbb{Z}/p_2^{f_1} \times \mathbb{Z}/p_2^{f_2} \\ &\times \mathbb{Z}/p_3^{g_1} \times \mathbb{Z}/p_3^{g_2} \times \mathbb{Z}/p_3^{g_3} \\ &\times \mathbb{Z}/p_4^{h_1}.\end{aligned}$$

For invariant factors: take rows (grouped by CRT)

$$\begin{aligned}&\mathbb{Z}/\left(p_1^{e_3} p_2^{f_2} p_3^{g_3} p_4^{h_1}\right) \\ &\times \mathbb{Z}/\left(p_1^{e_2} p_2^{f_1} p_3^{g_2}\right) \\ &\times \mathbb{Z}/\left(p_1^{e_1} p_3^{g_1}\right).\end{aligned}$$

Example 3.7.5 ***(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 3.7.6:

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

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 right-hand side below

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

Proposition 3.7.7 ***(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 3.7.8 ***(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 3.7.9: 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 3.7.10 ***(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 3.7.11 ***(?):*** 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 3.7.12 ***(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:

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

Crossing $[1,2]$ with everything:

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

And so on!

3.8 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 3.8.1 ***(Classification of groups of order*** p***).***
Every group G of prime order $p \geq 2$ is cyclic and thus isomorphic to $\mathbb{Z}/p$.

Proof (?).
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 3.8.2 ***(Classification of groups of order*** p^2***).***
Every group G of order p^2 is abelian, and thus isomorphic to either C_{p^2} or C_p^2.

Proof (?).
Quotient by the center to get $m := \#G/Z(G) \in \left\{1, p, p^2\right\}$. By cases:

- 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 3.8.3 ***(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 is cyclic and $G \cong S_p \times S_q \cong C_{pq}$.
2. If $q \mid p - 1$ then $G \cong S_q \rtimes_\psi S_p$ where $S_p \trianglelefteq G$ and $\psi : S_q \to \mathrm{Aut}(S_p)$, and G has a presentation

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

$$\ell \not\equiv 1 \bmod p \qquad \ell^q \equiv 1 \bmod p.$$

Proof (of pq theorem, case 1).

- Suppose $q < p$.
- Apply the Sylow theorems to p:

- $n_p \cong 1 \bmod p \implies n_p \in \{1, p+1, 2p+1, \cdots\}$.
- $n_p \mid q \implies n_p \in \{1, q\}$.
- Since $1 < q < p < p+1$, this forces $n_p = 1$

- Suppose $q \nmid p-1$ and apply the Sylow theorems to q:
  - $n_q \equiv 1 \bmod q \implies n_q \in \{1, q+1, 2q+1, \cdots\}$
  - $n_q \mid p \implies n_q \in \{1, p\}$
  - 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

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

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

  - 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 $G \coloneqq A \rtimes_\psi N$ 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:

$$\pi \curvearrowright A \rtimes_\psi N = A \rtimes_{\psi\circ\pi} N$$
$$f \curvearrowright A \rtimes_\psi N = A \rtimes_{\gamma_f\circ\psi} N.$$

  where

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

  - 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.

■

Lemma 3.8.4 ***(Frattini's Argument).***
If $N \trianglelefteq G$ and $P \in \operatorname{Syl}_p(H)$ then $G = N_G(P)H$.

Proof (?).

- Let $g \in G$, then since $P \leq H \trianglelefteq G$ we have $gPg^{-1} \subseteq gHg^{-1} = H$.
- So $P' \coloneqq gPg^{-1} \in \operatorname{Syl}_p(H)$ for all g, and since Sylows in H are all conjugate, we can write $P' = h^{-1}Ph^{-1}$ for some $h \in H$.
- This says $hPh^{-1} = gPg^{-1}$ and thus $P = (g^{-1}h)P(h^{-1}g) = (h^{-1}g)^{-1}P(h^{-1}g)$.
- But then $g^{-1}h \in N_G(P)$ so $g \in N_G(P)H$.

■

Lemma 3.8.5 ***(p groups are solvable).***
Every finite p group is solvable.

Proof (?).

- By induction on k in $\#G = p^k$: if $\#G = p$ then G is abelian and automatically solvable.
- Inductively, for $\#G = p^k$, now consider $Z(G) \neq 1$ since we're in a p-group.
- If $G/Z(G)$ is abelian, use the general fact: H solvable and G/H solvable implies G solvable.
  - Here $Z(G)$ and $G/Z(G)$ are both abelian and thus solvable.
- Otherwise $G/Z(G)$ is a p-group of size p^{k-1} and thus solvable by hypothesis.

■

Lemma 3.8.6 ***(pq groups have normals the size of the biggest prime).***
If $\#G = pq$ with $p < q$ distinct primes, then G has a normal subgroup of size q.
This is immediate from Sylow theory: $[n_q]_q = 1, n_q \mid p, p < q$ forces $n_q = 1$.

Proposition 3.8.7 ***(PQR Theorem).***
If $|G| = pqr$ where $p < q < r$ are distinct primes then G is solvable.

Proof (?).
Idea:

- Get a normal subgroup R of order r, so $\#(G/R) = pq$.
- Get a normal subgroup Q_1 of order q in G/R, which corresponds to $Q \trianglelefteq G$ of order qr containing R. Note that $R \trianglelefteq Q$ since normality descends to subgroups.
- Now $G \to Q \to R \to 1$ is a subnormal series whose quotients are all cyclic and thus abelian:
  - $\#(G/Q) = pqr/qr = p$,
  - $\#(Q/R) = qr/r = q$,
  - $\#(R/1) = r$,

■

Remark 3.8.8: Proof of first claim: let $m \coloneqq \#G = pqr$, then G has a normal subgroup of order r.

- Claim: at least one of the Sylows for p, q, or r is normal.
  - If none of the Sylow p, q, r groups are normal, then $n_r \geq r$ and $n_p \geq q$. Counting the contributions from just $\mathrm{Syl}_q(G)$ and $\mathrm{Syl}_p(G)$ yields

$$n_q(q-1) + n_r(r-1) \geq pr(q-1) + pq(r-1) = pqr + p(qr - q - r).$$

  - If this is to be at most m, it must be that $qr - q - r$ is negative (since $p > 1$ and otherwise this would yield more than pqr elements).

  - But if this holds,

$$qr - q - r \leq 0 \iff q(r-1) \leq r \iff q \leq \frac{r}{r-1}.$$

    But $q > 2$ be assumption, and $1 \leq \frac{r}{r-1} \leq 2$ for any number r. ↯.

  - So there is one of S_p, S_q, S_r that is normal in G.

- Now if S_r is normal we're done, so suppose not and $n_r > 1$. Claim: we can get another subgroup of order r

  - Let N be the normal Sylow, so either $N \in \mathrm{Syl}_p(G)$ or $N \in \mathrm{Syl}_q(G)$.

  - Then G/N has order $r\ell$ for either $\ell = q$ or $\ell = p$ respectively.

  - In either case, $\ell < r$. Using the lemma, G/N has a normal subgroup of size r, say $R/N \leq G/N$.

  - Then by the subgroup correspondence theorem, R corresponds to a normal subgroup $R' \trianglelefteq G$ of size $r\ell$ with $r < \ell$.

  - Applying the same lemma to R' immediately yields a normal subgroup R'' of order r in R'

  - Now use that $R'' \operatorname{char} R'$ since Sylows are characteristic, and $R' \trianglelefteq G$, so $R'' \trianglelefteq G$ too.

3.9 Series of Groups

Definition 3.9.1 (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 3.9.2 (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 3.9.3 (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 3.9.4 ***(Jordan-Holder).***
Any two composition series of a group have the same length and isomorphic composition factors (up to permutation).

Definition 3.9.5 (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 3.9.6.
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 3.9.7 (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 3.9.8 (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 3.9.9 (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.

3.10 Solvability

Remark 3.10.1: A useful way to extract normal subgroups: let G act on literally anything by $\varphi : G \to \mathrm{Aut}(X)$. Then $\ker \varphi \trianglelefteq G$ is always a normal subgroup. Some examples:

- $G \curvearrowright G$ by $x \mapsto gx$.
- $G \curvearrowright \{H \leq G\}$ by $H \mapsto gH$ or $H \mapsto gHg^{-1}$.
- $G \curvearrowright \left\{\mathrm{Syl}_p(G)\right\}$ for a fixed p by $S_p \mapsto gS_pg^{-1}$.
- $G \curvearrowright H$ for $H \trianglelefteq G$ by inner automorphisms $h \mapsto ghg^{-1}$.

Definition 3.10.2 (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 3.10.3: If $G = \mathsf{Gal}(L/K)$ 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 3.10.4 ***(Characterization of Solvable).***
A group G is solvable iff its derived series terminates.

Theorem 3.10.5 ***(S_n is Almost Always Solvable).***
If $n \geq 4$ then S_n is solvable.

Fact 3.10.6
Some useful facts about solvable groups:

- 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 ***(Subring criteria).***
A subset $S \subseteq R$ is a subring iff

- $(S, +)$ forms an abelian subgroup (so closed under addition and contains inverses)
- $(S, \cdot)$ forms a submonoid (so closed under multiplication)

Proposition 4.0.2 ***(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 $I \cap J = IJ$.

Definition 4.0.3 (Ideal generated by a set)
The ideal **generated** by $\{a, b\}$ is defined as

$$\langle a, b \rangle \coloneqq Ra + Rb \coloneqq \left\{ r_1 a + r_2 b \;\middle|\; r_i \in R \right\}.$$

More generally for a set $S = \{s_k\}$,

$$\langle S \rangle \coloneqq \sum_{k=1}^{\#S} Rs_k \coloneqq \left\{ \sum r_k s_k \;\middle|\; r_k \in R, s_k \in S \right\}.$$

Example 4.0.4 *(?):*

- $\langle p, q \rangle = \langle \gcd(p, q) \rangle \trianglelefteq \mathbb{Z}$.

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 $R \in \mathsf{Ring}, S \leq R, I \in \operatorname{Id}(R)$, 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 $I \in \operatorname{Id}(R)$, the canonical quotient map $\varphi : R \to R/I$ induces a bijective correspondence:

$$\begin{aligned} \left\{ J \in \operatorname{Id}(R) \;\middle|\; J \supseteq I \right\} &\rightleftharpoons \operatorname{Id}(R/I) \\ J \coloneqq \varphi^{-1}(\overline{J}) &\hookleftarrow \overline{J} \\ J &\mapsto \overline{J} \coloneqq \varphi(J), \end{aligned}$$

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 $\overline{S} \coloneqq S/I$ 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 $xx^{-1} \coloneqq 1 \in I$ 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 $\iff$ $\mathfrak{m} \in \mathrm{mSpec}(R)$ is maximal.
- $R/\mathfrak{p}$ is an integral domain $\iff$ $\mathfrak{p} \in \mathrm{Spec}(R)$ is prime.
- R/J is reduced $\iff$ J is radical.

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

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

■

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 $xy = 0 \bmod \mathfrak{p}$ with $y \neq 0 \bmod \mathfrak{p}$, we can check

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

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

$$y \coloneqq b + \mathfrak{p} = 0 + \mathfrak{p} = 0 \bmod \mathfrak{p}.$$

$\implies$: 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 $x \notin \mathfrak{p} \iff x \ncong 0 \bmod \mathfrak{p}$. Setting $x \coloneqq a + \mathfrak{p}, y \coloneqq b + \mathfrak{p}$ yields

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

Since $R/\mathfrak{p}$ is a domain, assuming $x \neq 0 \bmod \mathfrak{p}$ we have $y = 0 \bmod \mathfrak{p}$, 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 $\mathfrak{m} + Rx = R = \langle 1 \rangle$.

4.3 Undergrad Review

Remark 4.3.1: Notation:

- $\langle a \rangle \coloneqq Ra \coloneqq \left\{ ra \;\middle|\; r \in R \right\}$ 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 $K \coloneqq \mathbb{Q}(\zeta)$, 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 $R[[x_1, x_2, \cdots, x_n]]$.
- $\mathbb{Z}_p \coloneqq \left\{ a/b \;\middle|\; p \nmid b \right\}$ 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:

- $\ker f \coloneqq f^{-1}(\{0\})$.
- 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, $x \equiv y \bmod I \iff x - y \in I$.

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. $\sum_{i=1}^{n} 1_R = 0_R$.

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 irreducible $\implies$ prime, so this is an iff.

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):***

- $\mathrm{Id}(\mathbb{Z}) = \left\{ \langle m \rangle \;\middle|\; m \in \mathbb{Z}^{\geq 0} \right\}$
- $\mathrm{mSpec}\,\mathbb{Z} = \left\{ \langle p \rangle \;\middle|\; p \neq 0 \text{ is prime} \right\}$
- $\mathrm{Spec}\,\mathbb{Z} = \mathrm{mSpec}\,\mathbb{Z} \cup \{\langle 0 \rangle\}$.
- For k a field and $f \in k[x_1, \cdots, x_n]$ irreducible, $\langle f \rangle \in \mathrm{Spec}\, k[x_1, \cdots, x_n]$.
  - $\mathfrak{m} := \left\{ f = \sum_I a_I x^I \in k[x_1, \cdots, x_n] \;\middle|\; a_0 = 0 \right\} \in \mathrm{mSpec}\, k[x_1, \cdots, x_n]$ (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. Take $R \coloneqq k[x,y]/\left\langle x^2 - y^3 \right\rangle \cong k[x^2, y^3]$, which is a domain, But here $[x^2] = [y^3]$ as equivalence classes where $[y^3]$ is irreducible since every element in $r \in R$ has $\deg_y(r) = 0, 3, 6, \cdots$. But $[y^3]$ is not prime since it divides $[x^2]$ but doesn't divide $[x]$.

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

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

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

Example 4.3.23 ***(Some counterexamples):*** Some examples. Reminder: maximal always implies prime, and for PIDs, prime *and nonzero* implies maximal. Maximals quotient to fields, primes to domains.

- Prime and maximal:
  - $p\mathbb{Z} \in \operatorname{Id}(\mathbb{Z})$. Maximal (and thus prime) since $\mathbb{Z}/p$ is a field and a domain.
  - $\langle 2, x \rangle \in \operatorname{Id}(\mathbb{Z}[x])$. Maximal (and thus prime) $\mathbb{Z}[x]/\langle 2, x \rangle \cong \mathbb{Z}/2$ is a field and a domain.
- Prime but not maximal:

  - $\langle 0\rangle \in \mathrm{Id}(\mathbb{Z})$, since $m\mathbb{Z} \supseteq \langle 0\rangle$ for any m.
  - $\langle x\rangle \in R[x]$ over any integral domain since $R[x]/\langle x\rangle \cong R$ is a domain (making it maximal), but R can be chosen not to be a field (making it non-prime).

- Not prime, not maximal:
  - $m\mathbb{Z} \in \mathrm{Id}(\mathbb{Z})$, since m composite implies $\mathbb{Z}/m$ is not a domain since it has nonzero zero divisors. For example, in $\mathbb{Z}/6$, $[3]$ is a zero divisors since $[2][3] = 0$.

- Useful examples:
  - $\mathrm{mSpec}\,\mathbb{Z} = \{p\mathbb{Z}\}$ and $\mathrm{Spec}\,\mathbb{Z} = \{p\mathbb{Z}\} \cup \langle 0\rangle$.
  - $\mathrm{mSpec}\,\mathbb{C}[x] = \left\{x - a \;\middle|\; a \in \mathbb{C}\right\}$, since over a PID $\langle\alpha\rangle$ is maximal iff α is irreducible, and over $\mathbb{C}$ irreducibles are degree 1.
  - $\mathrm{mSpec}\,k[x_1, \cdots, x_n] = \left\{\langle x - a_1, x - a_2, \cdots, x - a_n\rangle \;\middle|\; a_k \in k\right\}$.

- A ring with no maximal ideals: the Prüfer p-group $\mathbb{Z}(p^\infty) = \left\{\zeta_{p^k}\right\}_{k=1}^{\infty}$ with the trivial ring structure $xy = 0$. The subgroups are $H_k := \left\{\zeta_{p^k}\right\}$, which form an increasing chain that doesn't stabilize.

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

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

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:

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

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

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 $\text{Id}(A) = \{0, A\}$.
- 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.

4.4.1 The Big Ones

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 $\text{Spec}\, R \subseteq \text{mSpec}\, R$.

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 (Euclidean Domain)
An integral domain R is **Euclidean** if R admits a degree function $d : R \to \mathbb{Z}_{\geq 0}$ such that for

all $x, y \in R$ there exist $q, r \in R$ with $x = qy + r$ and either $f(r) < f(y)$ or $r = 0$.

4.4.2 Others

Definition 4.4.13 (Noetherian)
A ring R is **Noetherian** if the ACC holds: every ascending chain of ideals $I_1 \leq I_2 \cdots$ stabilizes in the sense that there exists some N such that $I_N = I_{N+1} = \cdots$.

Definition 4.4.14 (Reduced Ring)
A ring R is **reduced** if R contains no nonzero nilpotent elements.

Definition 4.4.15 (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** $\kappa \coloneqq R/\mathfrak{m}$.

Exercise 4.4.16 (?)
Show that if R is a nonzero ring where every element is either a unit or nilpotent, then R is local.

Exercise 4.4.17 (?)
Show that if $p \in \operatorname{Spec} R$ then $R\left[p^{-1}\right]$ is local.

Exercise 4.4.18 (?)
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 $I \subseteq N \coloneqq R \setminus R^\times$, 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 4.4.19 (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 4.4.20 (?)
Show that a Dedekind domain R is a PID iff R is a UFD.

Definition 4.4.21 (Valuation Ring)
A **valuation ring** is an integral domain R such that for every $x \in \mathrm{ff}(R)$, $x \in R$ or $x^{-1} \in R$.

Definition 4.4.22 (Discrete Valuation Rings)
A **discrete valuation ring** or **DVR** is a local PID with a *unique* maximal ideal.

Definition 4.4.23 (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 4.4.24: 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.

4.5 Comparing and Transporting Ring Types

Proposition 4.5.1 ***(Characterizations of Rings).***

- R a commutative division ring $\implies$ R is a field
- R a finite integral domain $\implies$ R is a field.
- $\mathbb{F}$ a field $\iff$ $\mathbb{F}[x]$ 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 4.5.2 ***(?):*** A polynomial ring over a PID is not necessarily a PID: take $\langle 2, x\rangle \trianglelefteq \mathbb{Z}[x]$.

Proposition 4.5.3 ***(Big chain of inclusions).***
Fields $\subset$ Euclidean domains $\subset$ PIDs $\subset$ UFDs $\subset$ Integral Domains $\subset$ Rings

Remark 4.5.4: Sketch proofs of the inclusions:

- Field $\implies$ Euclidean: given x, y we need to write $x = qy + r$, so just take $q = y^{-1}$ and $r = 0$.
- Euclidean $\implies$ PID: to divide is to contain, and the Euclidean algorithm terminates to yield a gcd. Alternatively, pick an element $a \in I$ of minimal degree. If $I \neq Ra$ pick $b \in Ra$ that a doesn't divide and write $b = aq + r$ with $d(r) < d(a)$. Then $r = b - aq \in I$. ↯

- PID $\implies$ UFD:
  - To get existence, use that PIDS are Noetherian, maximals are generated by irreducibles, and irreducibles are prime. Write $a = a_1 b_1$ a proper factorization to get a proper containment $\langle a \rangle \subset \langle a_1 \rangle$ that eventually stabilizes to yield an irreducible factor a_r. Use the same idea to write a as finitely many irreducible factors.
  - To get uniqueness, write $a = \prod p_i = \prod q_i$ as primes and divide everything over.

Example 4.5.5 ***(showing these inclusions are strict):***

- A Euclidean Domain that is not a field: $k[x]$ for k a field.
  - *Proof*: Use that k a field implies $k[x]$ is a PID, and PID implies UFD. But this is not a field since the element x is not invertible.
- A PID that is not a Euclidean Domain: $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.
  - *Proof*: complicated.
- A UFD that is not a PID: $\mathbb{Z}[x]$.
  - *Proof*: $\mathbb{Z}$ a UFD implies $\mathbb{Z}[x]$ is a UFD, but $\langle 2, x \rangle = 2\mathbb{Z}[x] + x\mathbb{Z}[x] = \left\{ \sum r_i x^i \;\middle|\; r_0 \in 2\mathbb{Z} \right\}$ is not principal. Why: if $\langle 2, x \rangle = \langle f \rangle$ and f is constant, then every polynomial in this ideal has even coefficients and thus misses $g(x) \coloneqq x$. Otherwise, $\deg f \geq 1$ and we miss 2, which has degree zero.
- 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*: $[2]_4$ is a zero divisor since $[2]_4[2]_4 = [0]_4$.

4.6 Radicals

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

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

so $x^n \in I \implies x \in \sqrt{I}$.
An ideal is **radical** iff $\sqrt{I} = I$.

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

Fact 4.6.4
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.

Exercise 4.6.5 (?)
Notation: let N or $N(R)$ be the set of nilpotents in R. Let ZD or $ZD(R)$ be the set of zero divisors. Let $U, U(R), R^\times$ be the units of R.

- Show that every nilpotent is either zero or a zero divisor.
  - Solution: $a^m = 0$ with $a \neq 0$ and $m > 1$, then $xx^{m-1} = 0$, so x^{m-1} is a nontrivial element annihilating x.
- Show that R commutative and unital and x nilpotent implies $1+x$ is a unit, and moreover $N + R^\times = R^\times$ (the sum of a nilpotent and unit is a unit).
  - Solution: expand $1/(1+x) = \sum_{k=0}^{\infty} (-x)^k = \sum_{k=0}^{n} (-x)^k := f(x)$, so $(1+x)f(x) = 1$. Now use that $RN = N$ since $x^n = 0$ implies $(rx)^n = rxrx \cdots rx = r^n x^n = 0$. Taking $n + u \in N + R^\times$, then $u + n = u^{-1}(1 + u^{-1}n) \in R^\times R^\times$ since $u^{-1}n \in N$ and $1 + u^{-1} \in R^\times$ by the first part.
- Show that $f(x) = \sum a_k x^k \in R[x]$ iff $f \in R[x]^\times \iff a_0 \in R^\times, a_{k>1} \in N$.
  - Solution: use that if a_k is nilpotent, $a_k x^k$ is nilpotent. Then a_0 a unit at $a_1 x$ nilpotent implies $a_0 + a_1 x$ is a unit, and inductively f is a unit. If f is a unit, take $fg = 1$ with $f = \sum_{k=0}^{n} a_k x^k$ and $g = \sum_{k=0}^{m} a_k x^k$. Write $fg(x) = \sum_{k=0}^{n+m} c_k x^k$ where $c_k = \sum_{j=0}^{k} a_j b_{k-j}$. Using $fg = 1$, $c_0 = a_0 b_0 = 1$ so a_0, b_0 are units, and proceed inductively by descending coefficients, checking that $a_n b_m$ is the $r = 0$ case.
- Show that $f(x) \in N(R[x]) \iff a_k \in N(R)$ for all k.
  - Solution: f nilpotent with $f(x) = \sum a_k x^k$ implies $f^m = 0$, and check the leading term $a_n^m x^{nm}$. Induct down: $f, a_n x^n$ nilpotent implies $f - a_n x^n$ nilpotent. Conversely, if $a_i^{n_i} = 0$, use that $N(R) \trianglelefteq R$ form an ideal.
- Show that $f \in ZD(R[x]) \iff f \neq 0$ and $rf(x) = 0$ for some $r \in R$.

Definition 4.6.6 (Nilradical)
The **nilradical** of $R \in \mathsf{CRing}$ is

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

Exercise 4.6.7 (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. $N \coloneqq n + m - 1$.

- $R/\sqrt{0_R}$ 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

$$\bar{r}^n = 0 \bmod \sqrt{0_R} \iff \overline{r^n} \equiv 0 \bmod \sqrt{0_R} \iff r^n \in \sqrt{0_R} \iff r \in 0_R.$$

Exercise 4.6.8 (?)
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 $f \notin P$.

Definition 4.6.9 (Jacobson Radical)

The **Jacobson radical** $J(R)$ is the intersection of all maximal ideals, i.e.

$$J(R) = \bigcap_{\mathfrak{m} \in \mathrm{mSpec}\, R} \mathfrak{m}.$$

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

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

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

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

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

Exercise 4.9.9 (?)

- Show that in a PID, every element can be written as a finite product of irreducibles.

- Show that in a PID, every maximal ideal is generated by an *irreducible* element.
- Show that any PID is Noetherian.
- Show that not $\mathbb{Z}$ is Noetherian but not Artinian.
  - Hint: take a chain $n\mathbb{Z} \supseteq n^2\mathbb{Z} \supseteq \cdots$.

Exercise 4.9.10 (?)
Show that $R[x]$ a PID $\iff$ R is a field.

Solution:
Hint: take $r \in R$, then $\langle r, x\rangle = \langle f\rangle$ for some f. Write $r = fp$ and $x = fq$ for $p, q \in R[x]$, show $\deg f = 0$ and $\deg q = 1$. Write $f = c$ a constant, $q(x) = ax + b$ to get $c(ax + b) = x \implies ca = 1 \implies c \in R^\times \implies \langle f\rangle = R[x]$. Conclude by writing $1 = ar_1(x) + xr_2(x)$, evaluate at $x = 0$ to get $a^{-1} = r_1(0)$.

5 Number Theory

Proposition 5.0.1 ***(Properties of the norm).***
Let K be a number field and $N : K \to \mathbb{Z}$ be its norm function.

- $N(ab) = N(a)N(b)$
- $a \mid b \in K \implies N(a) \mid N(b) \in \mathbb{Z}$.
- $a \in K^\times \iff N(a) = \pm 1$.

6 General Field Theory

Remark 6.0.1: The most useful tricks of the trade:

- $\#\mathbb{G}_m(\mathbb{GF}(p^k)) = p^k - 1$, since every element is invertible except 0. You can use this to cook up strong numerical constraints on orders of elements. E.g. if $a^{17} = 1$ in some finite field of size p^k, $o(a)$ divides 17 and $o(a)$ divides $p^k - 1$, so $o(a)$ divides $\gcd(17, p^k - 1)$.
- Multiplicativity in towers can force numerical divisibility constraints. E.g. if α is a root of any irreducible f, take the tower $\mathrm{SF}(\alpha, k)/k(\alpha)/k$: then the degree of $\min_{\alpha,k}(x) \in k[x]$ divides the degree of the extension $[\mathrm{SF}(\alpha, k) : k]$.
-

6.1 Basics: Polynomials

Definition 6.1.1 (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.

Definition 6.1.2 (Primitive Polynomials)
For R a UFD, a polynomial $p \in R[x]$ is **primitive** iff the greatest common divisors of its coefficients is a unit.

Theorem 6.1.3 ***(Gauss' Lemma).***
Let R be a UFD and F its field of fractions. Then a primitive $p \in R[x]$ (so e.g. p monic) is irreducible in $R[x] \iff p$ is irreducible in $F[x]$.
More precisely, if $p = AB$ is reducible in $F[x]$, then there exist $r, s \in F$ such that $rA, sB \in R[x]$ and $p = (rA)(sB)$ is a factorization in $R[x]$.

Corollary 6.1.4.
A primitive polynomial $p \in \mathbb{Q}[x]$ is irreducible $\iff p$ is irreducible in $\mathbb{Z}[x]$.

6.2 Definitions

Definition 6.2.1 (Characteristic)
The **characteristic** of a ring R is the smallest integer p such that $\sum_{k=1}^{p} 1 = 0$.

Proposition 6.2.2 ***(Freshman's Dream).***
If $\operatorname{ch} k = p$ then $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$.

Definition 6.2.3 (Fixed Field)
For $H \leq \underset{\mathsf{Fields}_k}{\operatorname{Aut}}(L)$,

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

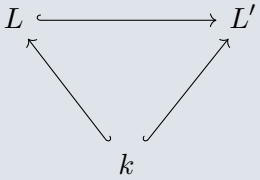
Definition 6.2.4 (Prime Subfield)
The **prime subfield** of a field F is the subfield generated by 1.

Theorem 6.2.5 ***(Characterization of Prime Subfields).***
The prime subfield of any field is isomorphic to either $\mathbb{Q}$ or $\mathbb{F}_p$ for some p.

Definition 6.2.6 (Field Automorphisms)

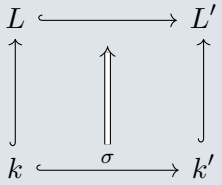
$$\mathrm{Aut}(L/k) = \left\{\sigma : L \to L \;\middle|\; \sigma|_k = \mathrm{id}_k\right\}.$$

Definition 6.2.7 (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:



Link to Diagram

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



Link to Diagram

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

Definition 6.2.8 (Perfect Fields)
The following are equivalent:

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

Example 6.2.9 ***(of a non-perfect field):*** Example of a non-perfect field: $\mathbb{F}_p(t)$. Use that $f(x) \coloneqq x^p - t$ is irreducible in $\mathbb{F}_p(t)[x]$ but not separable.

Proposition 6.2.10 ***(Characterization of perfect fields).***
k is perfect (using the irreducible implies separable condition) if either

- $\mathrm{ch}\, k = 0$ or
- $\mathrm{ch}\, k = p > 0$ and $k^p = k$.

Proof (?).
For $\operatorname{ch} k = 0$, use that irreducible implies separable.
For $\operatorname{ch} k = p$, show that $k_p \neq k \iff$ irreducible does *not* imply separable, so there exists an inseparable irreducible.

- Supposing $k^p \neq k$, choose $a \in k$ not a pth power.
- Note that $f(x) \coloneqq x^p - a$ has only one root in $\bar{k}$: in a splitting field, any root r satisfies $r^p = a$, so

$$x^p - a = x^p - r^p = (x-r)^p.$$

- Note f is irreducible: its only possible divisors are $(x-r)^m$ for $m \leq p$. Expanding yields

$$(x-r)^m = \sum_{k=0}^{m} \binom{m}{k} x^{m-k}(-r)^k = x^m + \binom{m}{1} x^{m-1}(-r)^m + \cdots,$$

  so the coefficient of x^{m-1} is $-mr \in k$.
- Thus if $(x-r)^m$ has a nontrivial divisor in $k[x]$ then m must be in $k^\times$, forcing $r \in k$. But then $r^p = a \in k$, ↯.

■

Remark 6.2.11 ***(Numerical Invariants):*** Let K/k be an extension.

$$[K:k] = \dim_{\mathsf{Vect}_k} K$$

is the dimension of K as a k-vector space. Automorphisms of fields over K are defined as

$$\operatorname*{Aut}_{\mathsf{Fields}_k}(K) \coloneqq \operatorname{Aut}(K/k) \coloneqq \left\{ \sigma : K \to K' \;\middle|\; \sigma|_k = \mathrm{id}_k \right\},$$

so lifts of the identity on k, and

$$\{K:k\} \coloneqq \#\operatorname{Aut}(K/k).$$

If K/k is finite, normal, and separable,

$$\mathsf{Gal}(K/k) \coloneqq \operatorname{Aut}(K/k),$$

where in general

$$\{K:k\} \leq [K:k]$$

with equality when L/k is Galois.

Fact 6.2.12

- 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 $\min(\alpha, k)$.

Proposition 6.2.13 ***(Towers are multiplicative in degree).***
Let $L/F/k$ be a finite tower of field extensions.

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

6.3 Finite Fields

Theorem 6.3.1 ***(Construction of Finite Fields).***
$\mathbb{GF}(p^n) \cong \frac{\mathbb{F}_p}{(f)}$ 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 6.3.2 ***(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 6.3.3 ***(Containment of Finite Fields).***
$\mathbb{GF}(p^\ell) \leq \mathbb{GF}(p^k) \iff \ell$ divides k.

Proposition 6.3.4 ***(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 .
Every element is a root by Cauchy's theorem, and the p^n roots are distinct since its derivative is identically -1.

todo

■

Proposition 6.3.5 ***(Splits Product of Irreducibles).***
Let $\rho_n \coloneqq x^{p^n} - x$. Then $f(x) \mid \rho_n(x) \iff \deg f \mid n$ and f is irreducible.

Corollary 6.3.6.
$x^{p^n} - x = \prod f_i(x)$ 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 6.3.7 ***(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

6.4 Cyclotomic Polynomials

Definition 6.4.1 (Euler's Totient Function)

$$\varphi(n) \coloneqq \#\left\{k \leq n \;\middle|\; \gcd(k, n) = 1\right\}.$$

Remark 6.4.2:

- $\varphi(p) = p - 1$, because every number $k \leq p - 1$ is coprime to p.

- $\varphi(p^k) = p^k - p^{k-1}$, since there are p^k total numbers less than p^k, most of which are coprime to p. The ones to remove are those dividing p^k: the only divisors of p^k are p^ℓ for $0 \leq \ell \leq k$, and $\gcd(p^k, m) = p^\ell$ whenever $m = tp$ for $t = 1, 2, 3, \cdots, p^{k-1}$ (i.e. m is divisible by some power of p, so the p^{k-1} multiples of p are possible).
- φ is multiplicative (arithmetically, so only on prime powers!)

Example 6.4.3 ***(Some totient values):***

$$\begin{aligned}\varphi(1) &= 1\\ \varphi(2) &= 1\\ \varphi(3) &= 2\\ \varphi(4) &= 2\\ \varphi(6) &= 2\\ \varphi(8) &= 4\end{aligned}$$

.

Definition 6.4.4 (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 6.4.5 (Cyclotomic Field)
Any subfield of $\mathrm{SF}(x^n - 1)$ is a **cyclotomic field**.

Proposition 6.4.6 ***(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.

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

so just use polynomial long division.

Fact 6.4.7 (computing cyclotomic polynomials, special cases and examples)

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

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

$$\Phi_1(z) = z - 1$$
$$\Phi_2(z) = z + 1$$
$$\Phi_4(z) = z^2 + 1$$
$$\Phi_6(z) = z^2 - z + 1$$
$$\Phi_8(z) = z^4 + 1.$$

Proposition 6.4.8 ***(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

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

Theorem 6.4.9 ***(Kronecker-Weber).***
If $K_{/\mathbb{Q}}$ is an abelian extension, then $K \subseteq \mathbb{Q}(\zeta_m)$ for some m.

6.5 Misc

Proposition 6.5.1 ***(?).***
If $f \in k[x]^{\text{irr}}$ with $\operatorname{ch} k = p$, then there is a unique separable $g \in k[x]^{\text{irr}}$ such that $f(x) = g(x^{p^k})$ for some unique k.

Definition 6.5.2 (Elementary Symmetric Functions)

todo

6.6 Exercises

Exercise 6.6.1 (?)
Show

$$x^\ell - 1 \mid x^m - 1 \iff \ell \mid m.$$

Solution:
$\implies$ - Write $m = \ell q + r$ with $0 \leq r < \ell$. - Write

$$p(x) = \frac{x^m - 1}{x^\ell - 1} = \frac{x^{lq+r} - 1}{x^\ell - 1} = x^r \frac{x^{lq} - 1}{x^\ell - 1} + \frac{x^r - 1}{x^\ell - 1} = q(x) + \frac{x^r - 1}{x^\ell - 1},$$

where p, q are polynomial by divisibility. - So the remaining ratio must be polynomial, but since $r < \ell$ is strict this forces $r = 0$. Thus $\ell \mid m$.
$\impliedby$:

- Write $m = \ell q + r$, then $r = 0$ by divisibility.
- Then $x^m - 1 = x^{\ell q} - 1 \coloneqq z^q - 1$ where $z \coloneqq x^\ell$.
- Use that $z - 1 \mid z^q - 1$, so $x^\ell - 1 \mid x` - 1 = x^m - 1$.

Exercise 6.6.2 (?)
Show that if $f \in \mathbb{F}_p[x]^{\text{irr}}$ is degree d,

$$f \mid x^{p^n} - x \iff d \mid n.$$

Solution:
$\impliedby$:

- If $d \mid n$, $x^d - 1 \mid x^n - 1$ by a previous exercise, and so $p^d - 1 \mid p^n - 1$.
- So $x^{p^d-1} \mid x^{p^n-1}$, now multiply through by x.
- Claim: $f \mid x^{p^d-1}$, from which the result immediately follows.
- For α any root of f, $\mathbb{F}_p(\alpha)$ is a finite field of size p^d since $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = d$.
- So $\mathbb{F}_p(\alpha) \cong \mathbb{GF}(p^d)$, which is the splitting field of $x^{p^d} - x$.
- Thus α is a root of $x^{p^d} - x$. Iterating over all roots yields the divisibility statement.

$\implies$:

- If $f \mid g_n(x) \coloneqq x^{p^n} - x$, then every root α of f is a root of g_n.
- So $\mathbb{F}_p(\alpha) \subseteq \mathbb{GF}(p^n)$.
- The result follows from the computation

$$\begin{aligned} n &= [\mathbb{GF}(p^n) : \mathbb{F}_p] \\ &= [\mathbb{GF}(p^n) : \mathbb{F}_p(\alpha)] \cdot [\mathbb{F}_p(\alpha) : \mathbb{F}_p] \\ &= kd. \end{aligned}$$

7 | Field Theory: Extensions and Towers

7.1 Basics

Remark 7.1.1: Galois is defined as **normal and separable**.

Definition 7.1.2 (Simple Extensions)
An extension L/k is **simple** iff $L = K(\alpha)$ for some $\alpha \in L$.

Theorem 7.1.3 ***(Primitive Element Theorem).***
Every finite separable extension is simple.

Corollary 7.1.4.
$\mathbb{GF}(p^n)$ is a simple extension over $\mathbb{F}_p$.

Definition 7.1.5 (Algebraic Extension)
A field extension L/k is **algebraic** iff every $\alpha \in L$ is the root of some polynomial $f \in k[x]$.

Theorem 7.1.6 ***(Finite Extensions are Algebraic).***
Every finite extension is algebraic.

Proof (that finite extensions are algebraic).
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.

■

7.2 Normal Extensions

Definition 7.2.1 (Normal Field Extension)
Let L/k be an extension. Then TFAE:

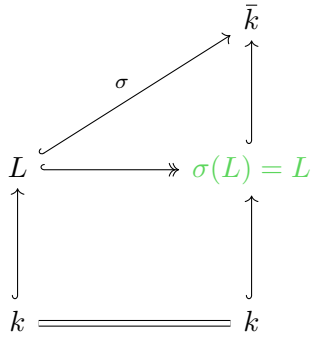
- L/k is **normal**.
- Every irreducible polynomial $f \in k[x]$ that has one root in L has *all* of its roots in L, and thus splits in $L[x]$.

– 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.

Example 7.2.2 ***(of normal extensions):***

- Useful trick: if $[L : k] = 2$ then L/k is automatically normal.
- Useful trick: if $L/K/k$, then K/k is normal iff $\mathsf{Gal}(L/K) \trianglelefteq \mathsf{Gal}(L/k)$.
- $K \coloneqq \mathbb{Q}(2^{\frac{1}{3}})$ is not normal, since $K \subset \mathbb{R}$ but $(x^3 - 2) = \prod_k x - \zeta_3^k 2^{\frac{1}{3}}$ with $\zeta_3, \zeta_3^2 \in \mathbb{C}$.
  - Another reason: an embedding $\sigma : K \to \bar{k}$ can send $2^{\frac{1}{3}}$ to any other root of $x^3 - 2$.
- $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is normal over $\mathbb{Q}$, since it it is finite and splits $f(x) \coloneqq (x^2 - 2)(x^2 - 3)$, which is a separable polynomial.
- $L \coloneqq \mathbb{Q}(2^{\frac{1}{4}})$ is not normal, since it is finite but not the splitting field of any polynomial.
- $\mathbb{Q}(\zeta_k)$ is normal for ζ_k any primitive kth root of unity.
- A normal non-separable extension: $\mathbb{F}_p(x, y)_{/\mathbb{F}_p(x^p, y^p)}$. This has finite degree p^2 but infinitely many subfields?

Proposition 7.2.3 ***(Characterization of normal algebraic extensions).***
For L/k algebraic: let $\bar{k}$ be an algebraic closure containing L, then L/k is normal iff every k-embedding $\sigma : L \to \bar{k}$ satisfies $\operatorname{im}\sigma = L$, so σ is a k-automorphism of L:



Link to Diagram

Definition 7.2.4 (Normal Closure)
If K/k is algebraic, then there is an extension N_k/K such that N_k/k is normal and $N_k/K/k$ is a tower. N_k is referred to as the **normal closure** of K/k.

Proposition 7.2.5 ***(Characterization of finite normal extensions as splitting fields).***
An extension L/k is finite and normal $\iff$ L is the splitting field of some polynomial $f \in k[x]$.

Proof (?).
$\implies$:

- Write $L = k(a_1, \cdots, a_n)$ by finiteness.
- Let m_i be the minimal polynomials of the a_i.
- By normality, the m_i split in $L[x]$.
- Then L is the splitting field of $f(x) \coloneqq \prod_i m_i(x)$.

$\impliedby$:

- Suppose $L/k = \mathrm{SF}(f)$, and pick any monic $m \in L[x]^{\mathrm{irr}}$ with a root $a \in L$, so that m is the minimal polynomial of a.
- Toward showing m splits in L: let $M = \mathrm{SF}(m)$, we'll show $M = L$.
- To show that for any root $b \in M$ we have $b \in L$, it suffices to show $[L(b) : L] = 1$.

  The strategy: use that $[L(a) : L] = 1$ since $a \in L$ by assumption, and try to relate the two degrees.
- We have L/k, and a number of towers to work with:

$$[L(a) : k] = [L(a) : k(a)][k(a) : k] \qquad = [L(a) : L][L : k]$$

$$[L(b) : k] = [L(b) : k(b)][k(b) : k] \qquad = [L(b) : L][L : k].$$

- In the first set of equalities, note that $k(a)_{/k} \cong k(b)_{/k}$ since a, b are conjugate roots over k. Moreover $L(a)_{/k(a)} \cong L(b)_{/k(b)}$ since both are splitting fields for f.
- Thus $[L(a) : k] = [L(b) : k]$, which forces $[L(a) : L] = [L(b) : L]$ after dividing by $[L : k]$. But $[L(a) : L] = 1$.

■

Proposition 7.2.6.
$|\mathrm{Aut}(L/k)| \leq [L : k]$ with equality precisely when L/k is normal.

7.3 Separable Extensions

Definition 7.3.1 (Separable polynomials)
A polynomial $f \in k[x]$ is **separable** iff f has no repeated roots.

Example 7.3.2 ***(of separable and inseparable polynomials):***

- $x^2 - 1$ is separable over $\mathbb{Q}$, but inseparable over $\mathbb{F}_2$ since it factors as $(x-1)^2$.
- $(x^2 - 2)^2$ is inseparable over $\mathbb{Q}$

- $x^2 - t$ is inseparable over $\mathbb{F}_2(t)$.
- $f(x) \coloneqq x^n - 1$ is inseparable over $\mathbb{F}_p$ when $p \mid n$.
  - Otherwise, $f' = nx^{n-1}$ has only $x = 0$ as roots, whereas 0 is not a root of f, so f is separable.
- $f(x) \coloneqq x^p - t$ is not separable over $\mathbb{F}_p(t)$: it is irreducible by Eisenstein, but has only the single root $t^{\frac{1}{p}}$.
- $f(x) \coloneqq x^{p^n} - x$ is separable over $\mathbb{F}_p$, since $f'(x) = -1$ has no roots at all.

Definition 7.3.3 (Separable Field Extension)
Let L/k be a field extension, $\alpha \in L$ be algebraic over k, and $f(x) \coloneqq \min(\alpha, k)$. The following are equivalent

- L/k is a **separable** extension.
- Every element $\alpha \in L$ is separable over k, so α has separable minimal polynomial $m(x)$ in some splitting field of m.
- Every finite subextension L'/k is separable.

Fact 7.3.4
If $\alpha \in K/k$ is separable, then α is separable in any larger field $L/K/k$ since the minimal polynomial over the larger field will divide the minimal polynomial over the smaller field.

Proposition 7.3.5 ***(Separability test:*** gcd ***with derivative).***
f is separable iff $\gcd(f, f') = 1$, so f, f' share no common roots. Moreover, the multiple roots of f are precisely the roots of $\gcd(f, f')$.

Proof (of separability test).
$\not\Longrightarrow$: Suppose f has a repeated root r_i, so its multiplicity is at least 2. Then

$$f(x) = (x-r)^2 g(x) \implies f'(x) = 2(x-r)g(x) + (x-r)^2 g'(x),$$

so r is a root of f'.
$\not\Longleftarrow$: Suppose r is a root of f, f'. Write $f(x) = (x-r)p(x)$ and $f'(x) = (x-r)p'(x) + p(x)$. Rearranging, $f'(x) - (x-r)p'(x) = p(x)$, and since r is a root of the LHS it's a root of the RHS. So $p(x) = (x-r)q(x)$ and $f(x) = (x-r)^2 q(x)$, making r a repeated root.
■

Proposition 7.3.6 ***(Separability test: identically zero derivative).***
$f \in k[x]^{\text{irr}}$ is **inseparable** (so f has a repeated root) iff $f'(x) \equiv 0$.

Proof (of separability test).
Assume f is monic, then f is inseparable iff f, f' have a common root a. So $(x-a) \mid q \coloneqq \gcd(f, f')$, and since f is irreducible, it must be the minimal polynomial of a. Since $f'(a) = 0$, this forces $f' \mid f$, and since $\deg f' = \deg f - 1 < \deg f$ this forces $f' \equiv 0$.
■

Proposition 7.3.7 ***(Derivative completely detects separability).***

- For any field k, $f \in k[x]$ is separable $\iff f' \not\equiv 0 \in k[x]$.
- For $\operatorname{ch} k = 0$, irreducible implies separable.
- For $\operatorname{ch} k = p$, irreducibles $f(x)$ are inseparable iff $f(x) = g(x^p)$ for some $g \in k[x]$.

Thus for an irreducible polynomial f,

$$f \text{ separable} \iff \gcd(f, f') = 1 \iff f' \not\equiv 0 \iff {}_{\operatorname{ch} k = p} f(x) = g(x^p).$$

Proof (?).

- First part:
  - $\not A \implies \not B$:
    - ♢ Let f be irreducible, and suppose f is separable. If $d(x) \coloneqq \gcd(f, f') \neq 1$, then f' can not divide f since f is irreducible, so f divides f'. But $\deg f' < f$ and $f \mid f'$ forces $f' \equiv 0$.
  - $\not B \implies \not A$:
    - ♢ If $f' \equiv 0$, then $d(x) \coloneqq \gcd(f, f') = \gcd(f, 0) = f \neq 1$ and f is *not* separable.
- Second part:
  - If $\operatorname{ch} k = 0$ and f is irreducible, then $\deg f \geq 2$ and $\deg f' \geq 1$ so $f' \neq 0$ and f is thus separable.
- Third part:
  - $\impliedby$: If $f(x) = g(x^p)$ then $f'(x) = g'(x^p) \cdot p x^{p-1} \equiv 0$.
  - $\implies$: Let f be irreducible and inseparable, so $f' \equiv 0 \in k[x]$. Then $f(x) \coloneqq \sum_{k=0}^{n} a_k x^k$ implies $f'(x) \coloneqq \sum_{k=1}^{n} k a_k x^{k-1}$, which is zero iff $k a_k \equiv 0$ so p divides $k a_k$. So $a_k \not\equiv 0$ forces $p \mid k$, so $f = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots$.

■

Corollary 7.3.8 ***(Inseparable iff polynomial in characteristic powers).***
If $f \in k[x]^{\text{irr}}$ and $p \coloneqq \operatorname{ch} k > 0$, then f inseparable $\iff f(x) = q(x^{p^n})$ for some unique n.

Proof (of inseparable characterization).
$\implies$:
Use that f is inseparable iff $f' \equiv 0$. The claim is that $f' \equiv 0$ in characteristic p iff all exponents present in f are divisible by p. If $f' \equiv 0$, write

$$\begin{aligned} & f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \\ \implies & f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1 \\ & \equiv 0, \end{aligned}$$

which forces $i a_i = 0$ for all i. For any $a_i \neq 0$, this forces $i \equiv 0 \bmod p$, so a_i can only be nonzero

when $p \mid i$, so $i = kp$ for some k. So reindex to write

$$f(x) = a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_n x^{np} = \left(b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n\right)^p \in \bar{k}[x],$$

using $(c+d)^p = c^p + d^p$ in characteristic p, and taking $b_i \coloneqq a_i^{\frac{1}{p}} \in \bar{k}$ So $f' \equiv 0 \implies f(x) = q(x^p)$ where $q(t) \coloneqq \sum b_i t^i$.
$\impliedby$: If $f(x) = q(x^p)$ for some q, the previous calculation shows q has multiple roots, thus so does f, so f is inseparable.

■

Fact 7.3.9 (Irreducible implies separable in characteristic zero)
If $\operatorname{ch} k = 0$ and $f \in k[x]^{\text{irr}}$, then f is automatically separable.

Why this is true: assuming f is irreducible, $\gcd(f, f') = 1$ or f. It can't be f, since $f \mid f'$ would force $\deg f = \deg f' = 0$ and make f a constant. So this gcd is 1.

Fact 7.3.10 (Irreducible implies separable for perfect fields)

- Use that irreducible polynomial f must have distinct roots, by the argument above. (In fact, it is the minimal polynomial of its roots.)
- Toward a contradiction, suppose f is irreducible but inseparable.
- Then $f(x) = g(x^p)$ for some $g(x) \coloneqq \sum a_k x^k$.
- Since Frobenius is bijective, write $a_k = b_k^p$ for some b_k, then

  $$f(x) = \sum a_k x^{pk} = \sum b_k^p x^{pk} = \left(\sum b_k x^k\right)^p,$$

  making f reducible. ↯

Fact 7.3.11 (finite extensions of perfect fields are separable)
A finite extension of a perfect field is automatically separable, and one only needs to show normality to show it's Galois.

Proposition 7.3.12 ***(Simplifications of separability for finite extensions).***
If L/k is a finite extension, then, TFAE:

- L/k is separable.
- $L = k(\alpha)$ for α a separable element.
- $L = k(S)$ for S some set of separable elements

- $[L:K] = [L:K]_s$, i.e. the separable degree equals the actual degree.

$$[L:k] = \{L:k\} \coloneqq \#\underset{\mathsf{Fields}_k}{\mathrm{Aut}}(L).$$

Proposition 7.3.13 ***(Separable splitting fields are Galois).***
If L/k is separable, then

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

If L/k is a splitting field, then

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

Proposition 7.3.14 ***(Irreducible polynomials have separable splitting fields).***
Irreducible polynomials have distinct roots after passing to a splitting field.

Proposition 7.3.15 ***(Algebraic extensions of perfect fields are separable).***
If $\operatorname{ch} k = 0$ or k is finite, then every *algebraic* extension L/k is separable.

Proposition 7.3.16 ***(Irreducible implies separable for perfect fields).***
If k is a perfect field, then every irreducible $f \in k[x]^{\mathrm{irr}}$ is automatically separable.

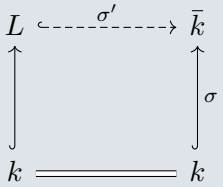
Proof (?).
If $\operatorname{ch} k = 0$ and f is irreducible, then since $\deg f' < \deg f$ and f is irreducible we must have $\gcd(f, f') = 1$ and f is separable.
If $\operatorname{ch} k = p > 0$, then if f is irreducible and inseparable then $f(x) = g(x^p)$ for some g. Write $g(x) = \sum a_k x^k$, and since k is perfect, write $b_k \coloneqq a_k^{\frac{1}{p}}$, then

$$f(x) = \sum a_k x^{pk} = \sum b_k^p x^{pk} = \left(\sum b_k x^k\right)^p,$$

so f is reducible. $\lightning$.

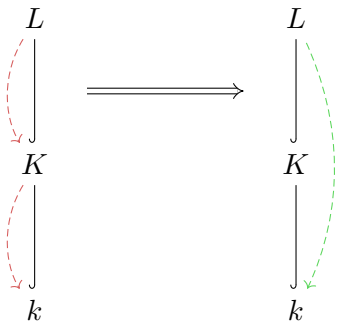
■

Definition 7.3.17 (Separable degree)
The **separable degree** of an extension L/k is defined by fixing an embedding $\sigma : k \hookrightarrow \bar{k}$ (the algebraic or separable closure) and letting $[L:k]_s$ be the number of embeddings $\sigma' : L \to \bar{k}$:



Link to Diagram

Proposition 7.3.18 ***(Separability is transitive.).***
If $L/K/k$, then L/K is separable and K/k is separable $\iff$ L/k is separable:



Link to Diagram

Proof (?).
Use that L/k is separable $\iff$ $[L:k] = [L:k]_s$.
$\Longleftarrow$:

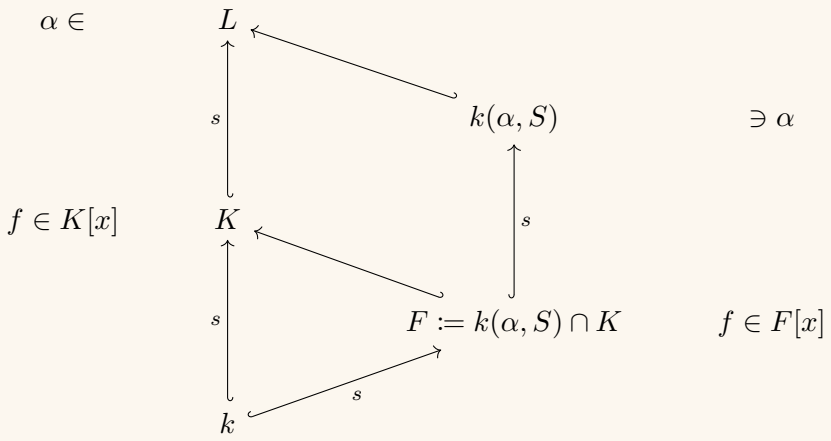
- By definition, every $\alpha \in L$ is separable over k.
- K/k is separable:
  - Since $K \subseteq L$, any $\alpha \in K$ is also separable over k.
- L/K is separable:
  - If $\alpha \in L$, then $\min\limits_{\alpha,k}(x)$ is a separable polynomial over some splitting field.
  - Use that L/k implies $\min\limits_{\alpha,L}(x)$ divides $\min\limits_{\alpha,k}(x)$, so the former is separable, done.

$\Longrightarrow$:

- Now use that the separable degree is multiplicative in towers.
- If all extensions in sight are **finite**, this direction is immediate:

$$[L:k]_s = [L:K]_s[K:k]_s = [L:K][K:k] = [L:K].$$

- For the infinite case, want to show every $\alpha \in L$ is separable over k. It suffices to show α is contained in some finite separable subextension. The strategy:



Link to Diagram

- Let $f(x) \coloneqq \min_{\alpha, K}(x)$ be the minimal polynomial of α *over the intermediate extension* K, which by assumption is separable since L/K is separable.
  - So $f \in K[x]$, and letting S be the finite set of coefficients of f, $S \subseteq K$.
  - Note that each coefficient $s \in S$ is separable over k since K/k is separable by assumption.
- Set $F \coloneqq k(\alpha, S) \cap K$. Note K/k is separable and $F \subseteq K$, so F/k is separable.
- Moreover $k(\alpha, S)/F$ is separable, since the minimal polynomial of α over F is still f.
- Now $k(\alpha, S)/F/K$ is a tower of finite extensions where $k(\alpha, S)/F$ and F/k are separable, so this reduces to the finite case.

■

Proposition 7.3.19 ***(Separability has the compositing property).***
E/k and F/k are separable $\iff$ EF/k is separable.

Proof (?).
$\impliedby$: Separability always descends to subfields, and $E \leq EF, F \leq EF$.
$\implies$:

- Write $E = k(S)$ for some finite set S. Then $EF = F(S)$.
- Use that $k(S)/k$ is separable iff $s \in S$ is a separable element for all s.
  - Since E/k is separable, each $s \in S$ is separable over k.
- Since F/k is separable, each $s \in S$ is separable over F.
- So $F(S)/F$ is separable.
- Now use the tower $F(S)/F/k$ to obtain $F(S)/k$ separable, which is EF/k.

■

7.4 Galois Extensions

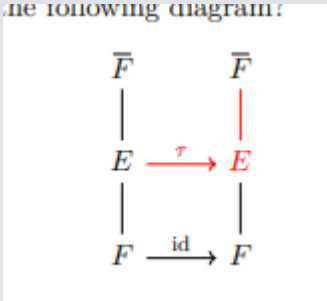
Definition 7.4.1 (Galois Extension and Galois Group)
Let L/k be a finite field extension. The following are equivalent:

- L/k is a **Galois extension**.
- L is normal, and separable.
- The fixed field L^H of $H \coloneqq \mathrm{Aut}(L/k)$ is exactly k.
- L is the splitting field of a separable polynomial $p \in K[x]$.
- L is a finite separable splitting field of an irreducible polynomial.
- There is a numerical equality:

$$\#\underset{\mathsf{Fields}_k}{\mathrm{Aut}}(L) = [L:k] = \{L:k\},$$

where $\{E:F\}$ is the number of isomorphisms to any field lifting id_F:

ne following diagram:

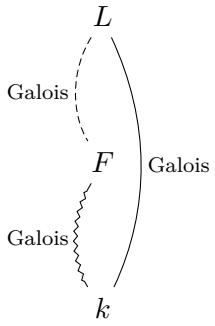


In this case, we define the **Galois group** as

$$\mathsf{Gal}(L/k) \coloneqq \underset{\mathsf{Fields}_k}{\mathrm{Aut}}(L/k).$$

Fact 7.4.2
For L/k algebraic and $\mathrm{ch}\, k = 0$, L/k is Galois $\iff$ L/k is normal.

Proposition 7.4.3 ***(Galois is upper transitive, characterization of when lower transitivity holds).***
If L/k is Galois, then L/F is **always** Galois. Moreover, F/k is Galois if and only if $\mathsf{Gal}(L/F) \trianglelefteq \mathsf{Gal}(L/k)$



Link to diagram

In this case,

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

Proposition 7.4.4 *(?).*
Let $L/K/k$ with L/k Galois. Then

$$K/k \text{ is Galois} \iff \mathsf{Gal}(L/K) \trianglelefteq \mathsf{Gal}(L/k),$$

and moreover $\mathsf{Gal}(K/k) = G$.

Proof (?).

- Note separability is distinguished, so K/k is separable.
- K/k is Galois $\iff$ F/k is normal (since we already have separability).
- $\iff$ $\sigma(K) = K$ for all $\sigma \in G$
- $\iff$ $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$.

So H is normal and G/H is a group. For the isomorphism, take

$$\begin{aligned} \rho : \mathsf{Gal}(L/k) &\to \mathsf{Gal}(K/k) \\ \rho &\mapsto \rho|_K. \end{aligned}$$

This is well-defined since by normality $\sigma(K) = K$. Any $f \in \ker \rho$ is the identity on K, so $f \in \mathsf{Gal}(L/K)$ and $\ker \varphi = H$. Since L/K is Galois, every $f \in \mathsf{Gal}(K/k)$ lifts to $\mathsf{Gal}(L/k)$, making ρ surjective.

■

Example 7.4.5 *(?):*

- $\mathbb{Q}(\zeta_3, 2^{1/3})$ 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.

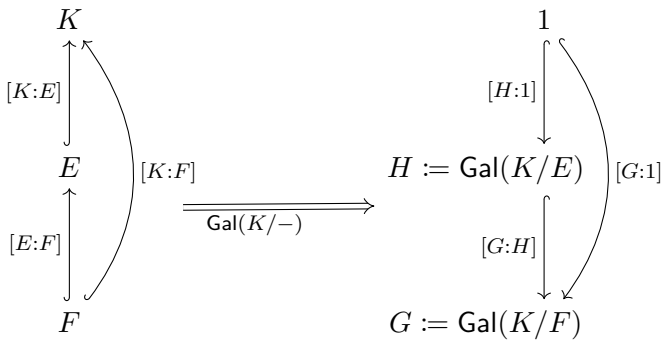
7.5 Fundamental Theorem of Galois Theory

Theorem 7.5.1 ***(Fundamental Theorem of Galois Theory).***
Let L/k be a Galois extension, then there is a correspondence:

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

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

Remark 7.5.2: A trick for remembering the degree/index correspondence:



Link to Diagram

Theorem 7.5.3 ***(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 7.5.4 ***(Composite Extensions).***
If F/k is finite and Galois and L/k is arbitrary, then FL/L is Galois and

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

7.6 Quadratic Extensions

Proposition 7.6.1 ***(Classification of quadratic extensions).***
If $\mathbb{F}$ is a field with $\operatorname{ch}(\mathbb{F}) \neq 2$ 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 7.6.2 ***(Quadratic extensions of rationals).***
If $E_{/\mathbb{Q}}$ is a quadratic extension, $E = \mathbb{Q}(\sqrt{q})$ for some $q \in \mathbb{Q}$ squarefree. Explicitly, use the primitive element theorem to write $E = \mathbb{Q}(\alpha)$, let f be the minimal polynomial, then take $q = b^2 - 4ac$. One can do slightly better by writing $b^2 - 4ac = a/b$ so that $\sqrt{b^2 - 4ac} = \sqrt{ab}/b$ and taking $q = ab$.

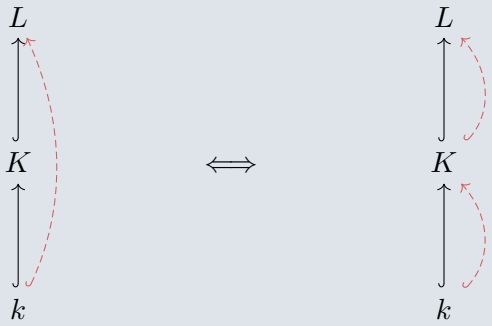
Proposition 7.6.3 ***(?).***
For $\mathbb{F}_p$ a finite field of prime order, all quadratic extensions $E/\mathbb{F}_p$ are isomorphic.

8 Distinguished Classes

See http://math.wsu.edu/students/jstreipel/notes/galoistheory.pdf

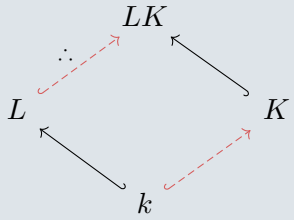
Definition 8.0.1 (Distinguished Classes)
A collection of field extensions $\mathcal{S}$ is **distinguished** iff

1. (Transitive property) For any tower $L/K/k$, the extension $L/k \in \mathcal{S} \iff L/K \in \mathcal{S}$ (upper transitivity) and $K/k \in \mathcal{S}$ (lower transitivity):



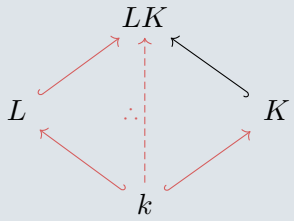
Link to Diagram

2. (Lifting property) Lifts of distinguished extensions are distinguished: $K/k \in \mathcal{S}$ and L/k any extension $\implies LK/L \in \mathcal{S}$:



Link to Diagram

3. (Compositing property) Whenever $L/k, K/k \in \mathcal{S}$, the amalgam $KL/k \in \mathcal{S}$ as well:



Link to Diagram

One is supposed to think of LK/L as a "lift" of K/k.

Example 8.0.2 ***(of distinguished classes):*** The following classes of extensions are distinguished:

- Algebraic.
- Finite.
- Separable.
- Purely inseparable.
- Finitely generated.
- Solvable.

⚠**Warning 8.0.3**
Normal extensions are *not* distinguished, since they fail the forward implication for (lower) transitivity. However, they do have the (forward implication) upper transitive, lifting, and compositing properties.

As a consequence, Galois extensions are also not distinguished.

Fact 8.0.4 (Normal/Algebraic/Galois extensions are upper transitive)
For $L/F/k$: L/k normal/algebraic/Galois $\implies$ L/F normal/algebraic/Galois.

8.0.1 Algebraic Extensions

Proposition 8.0.5 ***(Transitivity of algebraic extensions, forward implication).***
If $L/K/k$ (not necessarily finite) with L/K and K/k both algebraic, then L/k is algebraic.

Proof (?).

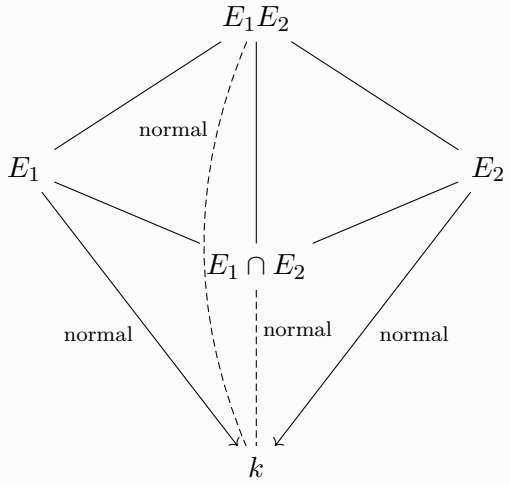
- We want to show every $\alpha \in L$ is algebraic over k, and it suffices to show α is algebraic over some finite subextension $k(S)$.
- Pick $\alpha \in L$, then α is algebraic over K by assumption, so it is a root of some $f \in K[x]$.
- Let S be the finitely many coefficients of f, then α is algebraic over $k(S)$.
- Note that $k(S)/k$ is finite and thus algebraic, and $k(S,\alpha)/k(s)$ is finite and also algebraic, so we're reduced to the finite case.
- It suffices to show $k(S,\alpha)/k(s)/k$ is finite, which follows from multiplicativity of degrees.

■

Remark 8.0.6: If $L/K/k$ with α algebraic over L, then α is algebraic over K and $\min_{\alpha,L}$ divides $\min_{\alpha,K}$ (so minimal polynomials only get smaller in extensions).

8.0.2 Normal Extensions

Corollary 8.0.7 ***(Normality satisfies the lifting property).***
E_1/k normal and E_2/k normal $\implies$ E_1E_2/k normal and $E_1 \cap E_2/k$ normal.



Link to diagram

Issues with Normal Towers

Example 8.0.8 ***(Normal extensions are not transitive: failure of lower transitivity, forward implication):*** One can similarly produce towers where the total extension is normal but the lower iterate is not normal: take

$$L/K/k := \mathbb{Q}(2^{\frac{1}{3}}, \zeta_3)/\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}.$$

Now K/k isn't normal, since $\mathsf{Gal}(L/k) = S_3$ but $\mathsf{Gal}(L/K) = \mathbb{Z}/2 \not\trianglelefteq S_3$.

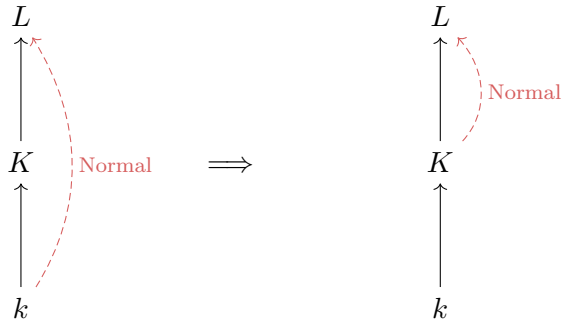
Another example: let L/k be any algebraic extension that isn't normal, and take N_k to be the normal closure to get N_k/L. Concretely, $N_{\mathbb{Q}}/\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}$ works.

Example 8.0.9 ***(Normal extensions are not transitive: failure of reverse implication):*** One can produce towers of successively normal extensions whose total extension is not normal in a cheap way: take

$$L/K/k := \mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}(2^{\frac{1}{2}})/\mathbb{Q}.$$

Each iterate is normal since it's quadratic, but the overall extension misses complex roots and is thus not normal.

Proposition 8.0.10 ***(Normal extensions are upper transitive, forward implication).*** For L/k finite,



Link to Diagram

Proof (Finite case).

- Use the fact that for finite extensions, L/k is normal and separable $\iff$ L is the splitting field of a separable polynomial $f \in k[x]$.
- Now regard f as a polynomial in $K[x]$; then L is still the splitting field of f over K, done.

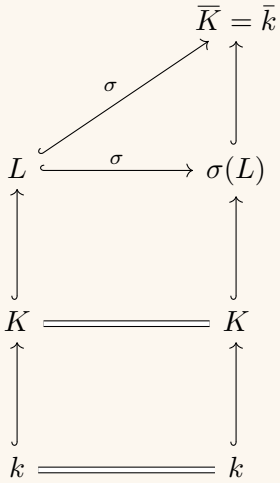
Alternatively,

- Let $\alpha \in L$ be a root of $f \in K[x]$ with f irreducible, it suffices to show all roots of f are in L.
- Let $m \in K[x]$ be the minimal polynomial of α over K, and let $m' \in k[x]$ be the minimal polynomial of α over k.
- Since L/k is normal and $\alpha \in L$, m' splits in L.
- Minimal polynomials are divisible in towers, so m divides m'. Since m' splits in L, so must m.

■

Proof (General case).

- Suppose $L/K/k$ with L/k normal, we want to show L/K is normal.
- Use the embedding characterization, it suffices to show that every embedding $\sigma : L \hookrightarrow \overline{K}$ satisfies $\operatorname{im}\sigma = L$:



Link to Diagram

- Now just use the fact that $\bar{k} = \overline{K}$, and since $k \subseteq K$, any K-morphism is also a k-morphism.
- Since L/k is normal, $\sigma(L) = L$ and L/K is thus normal.

■

9 | Galois Theory

Some useful exercises and solutions: https://feog.github.io/chap4.pdf

Remark 9.0.1:

- Given $x \coloneqq \sqrt{a} + \sqrt{b}$, to find a minimal polynomial consider $x^2, x^3, \cdots$ and try to get a linear combination. Then check if its irreducible.

  - General strategy here: try to isolate radicals on one side, then raise both sides to that power.

- To find a minimal polynomial for an element α, figure out the dimension of $\mathbb{Q}(\alpha)/\mathbb{Q}$ – say it's n, then $1, \alpha, \cdots, \alpha^n$ must be a $\mathbb{Q}$-linearly dependent set, so you compute these powers and fiddle with $\mathbb{Q}$ coefficients (or invert a matrix).

- Useful trick: for $x \coloneqq \sqrt{a} + \sqrt{b}$, compute x, x^2, x^3, x^4 and write them in terms of the basis $\left\{1, \sqrt{a}, \sqrt{b}, \sqrt{ab}\right\}$. Then put this linear system into a matrix and invert:

$$A\mathbf{v} = \mathbf{c} \coloneqq A\left[1, \sqrt{a}, \sqrt{b}, \sqrt{ab}\right] = \left[x, x^2, x^3, x^4\right].$$

Once you get $A^{-1}\mathbf{x} = \mathbf{b}$, read off the first row dotted against $\mathbf{b}$ to get a polynomial in x.

- In general: take α, sort out the degree n of the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$, and use the basis $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$.
- A trick to remember how degrees, indices and sizes match up: $L/K/F$ corresponds to $1/H/G$, and $[L:K] = [H:1] = \#H$, $[F:K] = [G:H]$, $[L:F] = [G:1] = \#G$, etc.
- Trick: once you find $\mathrm{SF}(f)/\mathbb{Q}$, if any subextension is not normal over $\mathbb{Q}$, then G can not be abelian.
  - Example: $f(x) = x^3 - 2$ splits in $\mathbb{Q}(\zeta_3, 2^{\frac{1}{3}})$ which is a non-normal extension $\mathbb{Q}(2^{\frac{1}{3}})$, forcing $G = S_3$.
- If $\alpha\beta \in \mathbb{Q}$, then $\alpha \in \mathbb{Q}(\beta)$ and vice-versa (I think).
- Checking subgroup lattices: https://hobbes.la.asu.edu/groups/groups.html
- De-nesting radicals:

- If you're denesting $\sqrt{a} - \sqrt{b}$, $a > b$.

Let's start with $\sqrt{a + \sqrt{b}}$. As you'll see in Example 3, the same method works if you replace the plus sign with a minus.

1. Assume that there exist some rational x and y such that
   $$\sqrt{a + \sqrt{b}} = \sqrt{x} + \sqrt{y}$$
2. Using the result from Wells, above, multiply by
   $$\sqrt{a - \sqrt{b}} = \sqrt{x} - \sqrt{y}$$
3. This yields
   $$\sqrt{a^2 - b} = x - y$$
4. Square the equation from step 1:
   $$a + \sqrt{b} = x + 2\sqrt{xy} + y$$
5. Set the rational parts equal:
   $$a = x + y$$
6. Solve the equations from steps 3 and 5 for x and y:
   $$x = \tfrac{1}{2}\left(a + \sqrt{a^2 - b}\right)$$
   $$y = \tfrac{1}{2}\left(a - \sqrt{a^2 - b}\right)$$

If the original nested radical has a minus sign, $\sqrt{a - \sqrt{b}}$, equations (1) and (2) come out exactly the same, so x and y are the same, but your answer is $\sqrt{x} - \sqrt{y}$.

Remark 9.0.2: Assume all extensions here are algebraic and finite. Let $f \in \mathbb{Q}[x]$ with $n := \deg f$.

Theorem 9.0.3 ***(The Algorithm).***

- Show your extension is Galois (normal and separable)
  - Show f is irreducible and separable.
- Find the degree of the extension d, since then $\#G = d$.
  - Note that in general, $G \leq S_n$ and $n \neq d$, $\#G \neq n$.
- Obtain $n \mid d \coloneqq \#G \mid n!$ and $G \leq S_n$ is a transitive subgroup, list possibilities.
- Rule out cases or determine the group completely by finding cycle types.

Example 9.0.4 ***(Of using the algorithm):*** Consider $f(x) \coloneqq x^5 - 9x + 3$, let $L \coloneqq \mathrm{SF}(f)/\mathbb{Q}$.

- f is irreducible: Apply Eisenstein with $p = 3$.
- f is separable:
  - $\mathbb{Q}$ is perfect, so irreducible implies separable.
- L is Galois:
  - $L/\mathbb{Q}$ is a finite extension over a perfect field and thus automatically separable.
  - $L/\mathbb{Q}$ is the splitting field of a separable polynomial, and thus normal.
- Since L is Galois, $\#G = d \coloneqq [L : \mathbb{Q}]$, so try to compute the degree by computing the splitting field (and its degree) explicitly.
  - Here: difficult! The roots are complicated.
- Since L is Galois, $G \leq S_5$ is a transitive subgroup. Possibilities:

$$S_5, A_5, F_5 \cong C_5 \rtimes C_4, D_5, C_5.$$

- Claim: $G = S_5$.
  - Reduce mod 2: $(x^2 + x + 1)(x^3 + x^2 + 1)$, yielding a cycle type $(2, 3)$. This rules out
    - C_5, D_5 since $3 \nmid 5, 10$.
    - A_5, since this is an odd number of even length cycles.
    - F_5 since $3 \nmid 20$.
  - So this only leaves S_5.

9.1 Showing Extensions are Galois

Fact 9.1.1
Showing your polynomial is irreducible:

- Eisenstein (including shifting/inverting tricks, see section below)
- To show f is irreducible, it suffices to show it is irreducible over any $\mathbb{F}_p[x]$.

- A quadratic with no real roots is irreducible.

Showing your polynomial is separable:

- Show directly that f has distinct roots in $\bar{k}$ by factoring it.
- For perfect fields, irreducibles are automatically separable.
- For f irreducible, f is separable iff $f'(x) \not\equiv 0$.

Showing your *extension* is separable:

- Splitting fields of separable polynomials are automatically separable *and* normal (and thus Galois).
- Algebraic extensions of a perfect field are automatically separable.
  - In particular, extensions over $\mathbb{Q}$ or any $\operatorname{ch} k = 0$ are separable, and one only needs to show normality.
- (Hard) Show $[L:k]_s = [L:k]$.
- (Hard) Use that separability is a distinguished class.

Showing your extension is normal:

- Show that L/k is finite and the splitting field of some separable polynomial.

Showing your extension K/k is Galois:

- Show normality and separability.
- Show K is the splitting field of a separable polynomial ("separable splitting field")
- Automatic when K/k is algebraic and a finite field, since it's the splitting field of $x^{p^n} - x$.

9.2 Irreducibility

Proposition 9.2.1 ***(Consequence of Chebotarev density: checking irreducibility mod p).***
If $f \in \mathbb{Z}[x]$ is monic and there exists any prime p such that $f \bmod p$ is irreducible in $\mathbb{F}_p[x]$, then f irreducible in $\mathbb{Q}[x]$.

Remark 9.2.2: Finding a good prime for this is hard, but irreducibility can be checked exhaustively in small fields: just enumerate all polynomials and try polynomial long division.

Example 9.2.3 ***(using irreducibility mod p):*** $f(x) \coloneqq x^4 + x + 1$ is irreducible in $\mathbb{Z}[x]$, since checking manually in $\mathbb{F}_2[x]$ shows that $0, 1$ are not roots mod 2 so there is not linear factor. Manually dividing $a_1x^2 + a_2x + a_3$ for $a_i \in 0, 1$ leaves remainders, so there are no quadratic factors.

Theorem 9.2.4 ***(Eisenstein's Criterion).***
If

$$f(x) = \sum_{i=0}^{n} \alpha_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x].$$

then f will be irreducible over $\mathbb{Q}[x]$ (and thus over $\mathbb{Z}[x]$ by Gauss' lemma) if $\exists p$ such that

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

Note that if f is monic, it suffices to find any prime dividing all of the non-leading terms.

Remark 9.2.5 ***(Shifting):*** If $f(x+a)$ satisfies Eisenstein for any p, then f is irreducible. This is generally because $\Delta_{f(x)} = \Delta_{f(x+a)}$, and if p works for Eisenstein on any f then $p \mid \Delta_f$.

Example 9.2.6 ***(of shifting):*** Set $f(x) \coloneqq x^2 + x + 2$, then $f(x+3) = x^2 + 7x + 14$ and Eisenstein applies at $p = 7$.

Remark 9.2.7 ***(Inverting):*** If $n \coloneqq \deg(f)$ and $x^n f(1/x)$ is irreducible, then f is irreducible. Note that this is just reversing the coefficients.

Example 9.2.8 ***(Of inverting):*** Take $f(x) \coloneqq 2x^5 - 4x^2 - 3$, then for $g(x) \coloneqq 3x^5 + 4x^2 - 2$ Eisenstein applies with $p = 2$.

Remark 9.2.9 ***(mod p reduction checks to find a good p for Eisenstein):*** If $f(x) \equiv b(x+a)^n \bmod p$ for some p where $n \coloneqq \deg f$, then Eisenstein may work on $f(x-a)$ using the prime p. Note the change in signs/reverse translation.

In other words, reduce mod p for various p, and if any p collapses f to a power of a linear factor, use that p for Eisenstein.

Example 9.2.10 ***(of mod p reduction checks):*** Check

$$f(x) \coloneqq x^3 + x^2 - 48x + 128 \rightsquigarrow f(x) \equiv (x-3)^3 \bmod 5,$$

and Eisenstein on $f(x+3)$ with $p = 5$ works.

9.3 Computing

9.3.1 Misc Useful Facts

Once you've confirmed that you have a Galois extension, some useful tricks are available:

Fact 9.3.1 (Degrees of extensions)

- The size $\#G(f)$ is the degree $[\mathrm{SF}(f) : \mathbb{Q}]$.
- The degree of $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is the degree of $\min_{\alpha}(x)$, or any irreducible polynomial with α as a root.
  - Note that $\mathbb{Q}(\alpha) \neq \mathrm{SF}(f)$ in general.
- If $f = \prod(x - r_i)$, then $\mathrm{SF}(f)$ contains every $\mathbb{Q}(r_i)$. Thus

$$[\mathbb{Q}(r_i) : \mathbb{Q}] = d \implies d \mid [\mathrm{SF}(f) : \mathbb{Q}].$$

  - Note that $d \neq \deg f$ in general!

Fact 9.3.2 (Random tricks)

- Reminder of rational roots test: for $f(x) = a_n x^n + \cdots + a_0$, rational roots are of the form p_0/p_n where $p_i \mid a_i$.
- $\mathsf{Gal}(L/k)$ permutes the roots of any irreducible polynomial in $k[x]$. In particular, if $L = \mathrm{SF}(f)$ with f reducible, then G must send roots of irreducible factors to conjugates of the same factor.
- $\mathbb{Q}(\zeta_a) = \mathbb{Q}(\zeta_b) \iff a = 2b$ and b is odd.
- If there are k complex conjugate pairs (accounting for $2k$ roots) then G contains a cycle $(1, 2)(3, 4) \cdots (2k - 1, 2k)$.
- If all exponents are even, $f(r) = 0 \iff f(-r) = 0$, so roots occur in pairs $(r, -r)$.
  - Pairs are preserved by G in the sense that every $\sigma \in G$ satisfies either $\{r, -r\} \mapsto \{r, -r\}$ or $\{r, -r\} \mapsto \{s, -s\}$ for another pair.
  - Example: $x^4 - 5x^2 + 5$ has two pairs.

9.3.2 Transitive Subgroups

Proposition 9.3.3 ***(Galois groups are transitive subgroups).***
If $f \in k[x]$ is irreducible, then $\mathsf{Gal}(\mathrm{SF}(f)/k) \leq S_n$ is **always** a transitive subgroup, i.e. it acts transitively on the set of roots.

Corollary 9.3.4.

$$n \mid \#\mathsf{Gal}(K/\mathbb{Q}) \mid n!.$$

Why: $\mathsf{Gal}(K/\mathbb{Q}) \cong G \leq S_n$, and Lagrange yields $\#H \mid n!$. Note that G acts on R the set of n roots, and since it acts transitively, R is a single orbit. By orbit stabilizer, $\mathcal{O}_r \cong G/\mathrm{Stab}_G(r)$ and thus

$$\#G = \#\mathcal{O}_r \cdot \#\mathrm{Stab}_G(r),$$

so both terms on the right-hand side patently divide $\#G$

Fact 9.3.5 (Table of transitive subgroups of S_n for qual-sized n)
Write C_n for the cyclic group of order n. The following are transitive subgroups of S_n for small n, where blue groups are nonabelian:

n in S_n	Transitive Subgroups	Sizes
1	1	1
2	$S_2 \cong C_2$	2
3	$S_3 \cong D_3, A_3 \cong C_3$	6,3
4	$S_4, A_4, D_4, C_4, C_2^2$	24,12,8,4,4
5	$S_5, A_5, F_5 \cong C_5 \rtimes C_4, D_5, C_5$	120,60,20,10,5

Other useful facts:

- $\#D_n = 2n$, $\#S_n = n!, \#A_n = n!/2$, and $\#F_5 = 20$.
- For degree 8 extensions (which sometimes arise as quadratic extensions of degree 4 extensions): $Q_8 \leq S_8$ is transitive and nonabelian of order 8, and has presentation

$$Q_8 = \left\langle \alpha, \beta \;\middle|\; \alpha^4 = \beta^4 = 1, \alpha\beta\alpha = \beta, \beta^2 = \alpha^2 \right\rangle.$$

  Note that $Q_8 \leq S_8$ but $Q_8 \not\leq S_{<7}$.
- F_5 has presentation

$$\left\langle a, b \;\middle|\; a^5, b^4, bab^{-1} = a^2 \right\rangle.$$

9.3.3 Distinguishing Groups

Material borrowed from https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisSnAn.pdf

Remark 9.3.6 ***(Distinguishing groups):***
By n in $G \leq S_n$:

$n = 4$:

- C_2^2 vs C_4:
  - C_2^2 has two elements of order 2, the latter does not. So a cycle of type $(2, 2)$ forces C_2^2.

- S_4 vs A_4:
  - S_4 contains a Sylow-2 subgroup of order 8 (which divides $4! = 24$) but A_4 does not since it's of order $4!/2 = 12$ and $8 \not| 12$.
  - If G contains a transposition, then $G = S_4$ or D_4, since A_4 doesn't contain a transposition.
- D_4 vs Q_8:
- 5 roots:
  - S_5 is generated by any transposition and any 5-cycle.
  - S_n is generated by (a, b) and $(1, 2, \cdots, n) \iff \gcd(b - a, n) = 1$. In particular, the $(1, 2)$ and any length n cycle works.

Fact 9.3.7 (Recognizing cycle types)
The following are the cycle types that can occur:

Type	S_4	A_4	D_4	$\mathbf{Z}/4\mathbf{Z}$	V
$(1,1,1,1)$	1	1	1	1	1
$(1,1,2)$	6		2		
$(2,2)$	3	3	3	1	3
$(1,3)$	8	8			
(4)	6		2	2	
Sum	24	12	8	4	4

TABLE 3.

-

Proposition 9.3.8 ***(Recognizing A_n or S_n).***
Useful fact: if $G \leq S_n$ for n prime contains a 2-cycle and a p-cycle, then $G \cong S_n$. Note that for n not prime, a transposition and an n-cycle isn't enough, since one needs the specific n-cycle $(1, 2, \cdots, n)$ in general.
If $n > 2$ and G contains a 3-cycle and an n-cycle, then $G = A_n$ or S_n. Note that by Orbit-Stabilizer $n \mid \#G$, and if n is prime then by Cauchy there is an n-cycle (but this is not always the case). In fact, it suffices to find a k-cycle for any $k \geq n/2$, which can be found by reducing mod p and examining cycle types.
Moreover, if G contains a 2-cycle (transposition), then $G = S_n$.

Remark 9.3.9 ***(Other useful facts to reason about A_n):***

- Alternating groups have even numbers of cycles of even length.
- Elements in A_n either have cycle type with an even number of even lengths (including 0).
- A_4 does not contain a subgroup isomorphic to C_2^2.

Fact 9.3.10
Some useful generating sets: see https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf

Group	Generating Set	Size	Where
S_n, $n \geq 2$	(ij)'s	$\frac{n(n-1)}{2}$	Theorem 2.1
	$(12), (13), \ldots, (1n)$	$n-1$	Theorem 2.2
	$(12), (23), \ldots, (n-1\ n)$	$n-1$	Theorem 2.3
	$(12), (12\ldots n)$ if $n \geq 3$	2	Theorem 2.5
	$(12), (23\ldots n)$ if $n \geq 3$	2	Corollary 2.6
	$(ab), (12\ldots n)$ if $(b-a, n) = 1$	2	Theorem 2.8
A_n, $n \geq 3$	3-cycles	$\frac{n(n-1)(n-2)}{3}$	Lemma 3.1
	$(1ij)$'s	$(n-1)(n-2)$	Theorem 3.2
	$(12i)$'s	$n-2$	Theorem 3.3
	$(i\ i+1\ i+2)$'s	$n-2$	Theorem 3.4
	$(123), (12\ldots n)$ if $n \geq 4$ odd	2	Theorem 3.5
	$(123), (23\ldots n)$ if $n \geq 4$ even	2	Theorem 3.5
$\mathrm{SL}_2(\mathbf{Z})$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	2	Theorem 4.1
$\mathrm{GL}_n(\mathbf{R}), \mathrm{SL}_n(\mathbf{R})$	Elementary Matrices	Infinite	Theorem 5.2

2 Generators for S

9.3.4 Density: Cycle Types

Proposition 9.3.11 ***(A consequence of Chebotarev Density: reading cycles from reduction mod p).***
For any $p \not| \Delta$, writing $f(x) = \prod_{i=1}^{m} f_i(x) \bmod p$, G contains a cycle of type $(\deg f_1, \deg f_2, \cdots, \deg f_m)$. Equivalently, if $\tilde{f} \coloneqq f \bmod p$, then $G(\tilde{f}) \leq G(f)$ is a subgroup.

⚠ Warning 9.3.12
Warning: this only works if the f_i are distinct, i.e. there are no repeated factors in the factorization $\bmod p$.

Example 9.3.13 ***(Ruling out choices by existence of cycle types):*** You can use this to rule out types of groups using Lagrange's theorem: if you find a cycle of length m which doesn't divide $\#H$, then H isn't a possibility! Example: $\deg f = 5$ with exactly one conjugate pair of roots, then there is a 5-cycle $\sigma \coloneqq (1, 2, 3, 4, 5)$ because $5 \mid \#G$ and a 2-cycle $\tau \coloneqq (1, 2)$ coming from complex

conjugation. There check that $a_1 \coloneqq \sigma\tau\sigma^{-1} = (1,5)$ and $a_1\tau = (1,5,2)$ is a 3-cycle, so $3 \mid \#G$. This rules out F_5 which is of order 20, since $3 \nmid 20$.

Example 9.3.14 ***(Finding cycle types by reducing mod p):*** Consider $f(x) = x^5 + 2x + 1$. Reducing to $\mathbb{F}_3$ yields no roots, so f is irreducible, and moreover $G(f)$ contains a 5-cycle. Reducing to $\mathbb{F}_7$ splits f as $(x+2)(x+3)(x^3+2x^2+5x+5)$, so $G(f)$ contains a 3-cycle.

Example 9.3.15 ***(of using density):*** Take $f(x) \coloneqq x^6 + x^4 + x + 3$, then

$$\begin{aligned} f(x) &\equiv (x+1)(x^2+\cdots)(x^3+\cdots) \bmod 2 &&\implies \text{type } (1,2,3) \in G \\ f(x) &\equiv x(x+2)(x^4+\cdots) \bmod 3 &&\implies \text{type } (1,1,4) \in G \end{aligned}$$

.

Example 9.3.16 ***(of using density):*** Take $f(x) \coloneqq x^4 + x + 1$, then

$$\begin{aligned} f(x) &\equiv x^4 + x + 1 \bmod 2 &&\implies \text{type } (4) \\ f(x) &\equiv (x-1)(x^3+x^2+x-1) \bmod 3 &&\implies \text{type } (1,3) \end{aligned}$$

.

So G contains a 4-cycle and a 3-cycle. This is enough to show $G = A_4$.

Example 9.3.17 ***(?):*** Let $f(x) = x^6 + x^4 + x + 3$, reduce $\bmod 11$ to get a cycle type $(1,5)$. So $G \leq S_6$ contains a 5-cycle, where $5 > n/2 \coloneqq 6/2 = 3$, meaning $G = A_n, S_n$. Now reduce $\bmod p$ for various p to look for a cycle type of the form $(2,1,1,\cdots)$ or $(3,1,1,\cdots)$. This is hard, but $f \bmod 2$ has type $(1,2,3)$ and $((a,b)(c,d,e))^3 = (a,b)$, so G contains a transposition and thus $G = S_n = S_6$.

Example 9.3.18 ***(?):*** Let $f(x) = x^7 - x - 1$, reduce $\bmod 2$ to get a 7-cycle, and $\bmod 3$ to get $(2,5)$. Then use $(2,5)^5 = (2,1,1,\cdots)$ to get a transposition, So $G = S_7$.

Example 9.3.19 ***(?):*** Let $f(x) \coloneqq x^7 - 7x + 10$. Reducing $\bmod 3$ yields $(2,5)$ and $(2,5)^5 = (2,\cdots)$ and have a transposition. Since $5 > n/2 = 7/2$, $G = S_7$.

9.3.5 Discriminants

Definition 9.3.20 (Discriminant)
For $f = \sum a_k x^k$ monic,

$$\Delta_f = \prod_{i<j} (r_i - r_j)^2.$$

Note that $\Delta = 0$ when f has a repeated root.
For cubics,

- $\Delta > 0 \implies$ 3 distinct real roots
- $\Delta < 0 \implies$ 1 real root and 1 conjugate pair.

Example 9.3.21 ***(How to actually write this product):*** For f a cubic:

$$\begin{aligned}\Delta_f = (r_1 - r_2)^2(r_1 - r_3)^2 \\ (r_2 - r_3)^2.\end{aligned}$$

For f a quartic:

$$\begin{aligned}\Delta_f = (r_1 - r_2)^2(r_1 - r_3)^2(r_1 - r_4)^2 \\ (r_2 - r_3)^2(r_2 - r_4)^2 \\ (r_3 - r_4)^2.\end{aligned}$$

In general, for a degree n polynomial this will have $n(n-1)/2$ terms.

Remark 9.3.22: In general,

$$G \subseteq A_n \iff \sqrt{\Delta} \in k,$$

i.e. Δ is a perfect square in the ground field k.

Some special cases of discriminant values:

- Quadratics:

$$f(x) = ax^2 + bx + c \implies \Delta = b^2 - 4ac.$$

- Cubics:
  - General:

$$f(x) = ax^3 + bx^2 + cx + d \implies \Delta = b\check{s}c\check{s} - 4ac\c{s} - 4b\c{s}d - 27a\check{s}d\check{s} + 18abc.$$

♢ Note that you can depress a general cubic by substituting $t = x - \dfrac{b}{3a}$, yielding

$$f(t) = t\c{s} + pt + q \implies \Delta = -4p\c{s} - 27q\check{s}.$$

Remark 9.3.23: Some useful facts:

- $\Delta = 0 \iff f$ has a repeated root.
- $G \hookrightarrow A_n \iff \Delta$ is a perfect square in k.

9.4 Worked Examples

Fact 9.4.1

Example 9.4.2 ***(Indirect: exactly one conjugate pair of roots):*** If $\deg f = 5$ with exactly 3 real roots and one non-real complex conjugate pair, then $G(f) = S_5$. G contains a transposition, namely complex conjugation on the conjugate pair. This already implies $G \neq A_5$, since a transposition is an odd number of even cycles.

The claim is that G contains an element of order 5, i.e. a 5-cycle, which is enough to generate S_5. This follows because

- Galois acts transitively, so there is a length 5 orbit.
- By Orbit-Stabilizer, 5 divides $\#G$.
- By Sylow, there is an element of order 5.

So $G = S_5$.

9.4.1 Quadratics

Example 9.4.3 ***(Classifying quadratics):*** 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 $L[x]$, so L is automatically a splitting field.
  - Why? $\alpha \in L \implies \min_{\alpha}(x) = (x-\alpha)g(x)$ which forces $\deg(g) = 1$.
- If $\mathrm{ch}(k) \neq 2$, then L is separable since

$$\min_{\alpha}(x)' = 2x + \cdots \not\equiv 0,$$

Remark 9.4.4: One can complete the square for quadratics:

$$f(x) = x^2 + \alpha x + \beta = \left(x - \frac{\alpha}{2}\right)^2 + \beta - \frac{\alpha^2}{4} \ . \ .$$

Thus it suffices to consider quadratics of the form $x^2 + a$.

Example 9.4.5 ***(Quadratics):***

- $G(x^2 - m) = C_2$ for m not a perfect square.
  - $x^2 - m = (x + \sqrt{m})(x - \sqrt{m})$, so the splitting field is $\mathbb{Q}(\sqrt{m})$ of degree 2.

  - Since $G \leq S_2$ and has order 2, $G = S_2 \cong C_2$.
  - Concretely, take $m = 2$, then $G = \{\mathrm{id}, \tau\}$ where $\tau : \sqrt{2} \mapsto -\sqrt{2}$, and correspondingly $a + b\sqrt{2} \mapsto a - b\sqrt{2}$.
- $G((x^2-2)(x^2-3)) = C_2 \times C_2$.
  - Since G must permute irreducible factors, labeling the roots $r_1, r_2 = \pm\sqrt{2}$ and $r_3, r_4 = \pm\sqrt{3}$, we have
$$G \subseteq \langle (1,2), (3,4) \rangle = \{\mathrm{id}, (1,2), (3,4), (1,2)(3,4)\} \cong C_2 \times C_2.$$
  - $\#G = 4$, taking the tower $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and noting $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ which makes each step degree 2. So this forces $G \cong C_2 \times C_2$.

9.4.2 Cubics

Remark 9.4.6: Tricks/reminders:

- Try the rational roots test to check irreducibility, since reducible implies there's a linear factor.
- Nice situation: one real and two complex roots. Try Calculus and MVT to reason about real roots. This immediately yields S_3.
- Otherwise, 3 real roots (or no easy way to check root types). Try discriminant classification: put in the form $t^3 + pt + q$, potentially using $t = x - b/3a$, then $\Delta = -4p^3 - 27q^2$.

Remark 9.4.7 ***(Easy cycles in odd/prime degrees with basic Calculus):*** If $n \coloneqq \deg f$ is odd, then f has at least one real root. If f has two non-real roots, then G contains a transposition. If n is prime, then G contains an n-cycle (by transitivity and Cauchy), forcing $G = S_n$.

Example 9.4.8 ***(Of using easy cycles to get S_3):*** Let $f(x) = x^3 - 2$.

Then $f'(x) = 3x^2$, so f is monotone increasing. By the MVT, checking $f(-2) < 0$ and $f(2) > 0$, f has a single real root in $[-2, 2]$. The other two must be a complex conjugate pair.

Alternatively, just factor the darn thing: $f(x) = (x - \omega)(x - \zeta_3\omega)(x - \zeta_3^2\omega)$ where $\omega \coloneqq 2^{\frac{1}{3}}$ and $\zeta_3^3 = 1$.

So $G(f)$ contains a transposition, and since $\deg f = 3$ is prime, G contains a 3-cycle and $G(f) = S_3$.

Example 9.4.9 ***(Of using easy cycles to get S_3):*** Let $f(x) = x^3 - 4x + 5$.

Then $f'(x) = 3x^2 - 4 = 0$ when $x = \pm\sqrt{4/3}$. Checking $f''(x) = 6x$ yields a max at $-\sqrt{4/3}$ and a min at $\sqrt{4/3}$. Checking

$$f(4/3) = (4/3)^3 - 4(4/3) + 5 = (64/27) - (16/3) + 5 = 55/27 > 0,$$

so knowing the general shape of a cubic, there is exactly one real root, somewhere in $(-\infty, -\sqrt{4/3})$. So $G(f) = S_3$.

Proposition 9.4.10 ***(Classification for cubics).***
Away from $\operatorname{ch} k = 2$, Galois groups of cubics are entirely determined by discriminants:
There are only two possibilities: S_3 or $A_3 \cong C_3$.

- If $\sqrt{\Delta} \in k$, then $G \cong A_3$.
- Otherwise, $G \cong S_3$.

$f(X)$	disc f	G
$X^3 - X - 1$	-23	
$X^3 - 3X - 1$	81	
$X^3 - 4X - 1$	229	
$X^3 - 5X - 1$	473	
$X^3 - 6X - 1$	837	

TABLE 1. Some Galois gr

Example 9.4.11 ***(of discriminants of cubics):***

$f(X)$	disc f	Roots
$X^3 - 3X - 1$	9^2	$r,\ r^2 - r - 2,\ -r^2 + 2$
$X^3 - X^2 - 2X + 1$	7^2	$r,\ r^2 - r - 1,\ -r^2 + 2$
$X^3 + X^2 - 4X + 1$	13^2	$r,\ r^2 + r - 3,\ -r^2 - 2r + 2$
$X^3 + 2X^2 - 5X + 1$	19^2	$r,\ r^2 + 2r - 4,\ -r^2 - 3r + 2$

TABLE 2. Some cubics with Galois group A_3 over $\mathbf{Q}$.

Example 9.4.12 ***(Cubics (manually)):***

- $G(x^3 + x + 1) = S_3$:
  - Irreducible because it has no rational roots (by the rational roots test)
  - $f'(x) = 3x^2 + 1 > 0$ so f increases everywhere and can only have one real root r, so $\mathbb{Q}(r)/\mathbb{Q} = \deg f = 3$.

- The other roots are a non-real conjugate pair $w, \overline{w}$, so $\mathbb{Q}(w,r)/\mathbb{Q}(r) = \deg f(x)/(x-r) = 2$.
- So $[\mathrm{SF}(f) : \mathbb{Q}] = 6$, and the only transitive subgroup of order 6 in S_3 is S_3 itself.

Example 9.4.13 ***(Cubics (using Δ)):***

- $G(x^3 - x + 1) = S_3$:
  - This is already a depressed cubic, so use $\Delta = -4(-1)^3 - 27(1) = -23$.
  - $\Delta = -23 \notin \mathbb{Q}^2$, so $G \not\leq A_4$ which forces $G = S_4$.
- $G(x^3 - 3x + 1) = A_3$:
  - This is already a depressed cubic, so $\Delta = -4(-3)^3 + 27(1) = -3(27) = 81$.
  - $\Delta = 81 \in \mathbb{Q}^2$, so $G \leq A_3$.

9.4.3 Quartics

Definition 9.4.14 (Resolvent of a quartic)
If

$$f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

then define the **resolvent** of f by

$$R_4(t) = t^3 - a_2t^2 + (a_1a_3 - 4a_0)\,t + 4a_0a_2 - a_1^2 - a_0{a_3}^2.$$

Alternatively, it can be defined in terms of the roots r_i:

$$(x - (r_1r_2 + r_3r_4))\,(x - (r_1r_3 + r_2r_4))\,(x - (r_1r_4 + r_2r_3))\,.$$

For depressed quartics,

$$f(X) = X^4 + cX + d \Longrightarrow R_3(X) = X^3 - 4dX - c^2.$$

Proposition 9.4.15 ***(Classification for quartics).***
The Galois groups of irreducible quartics can be determined using discriminants, resolvents, and checking irreducibility:

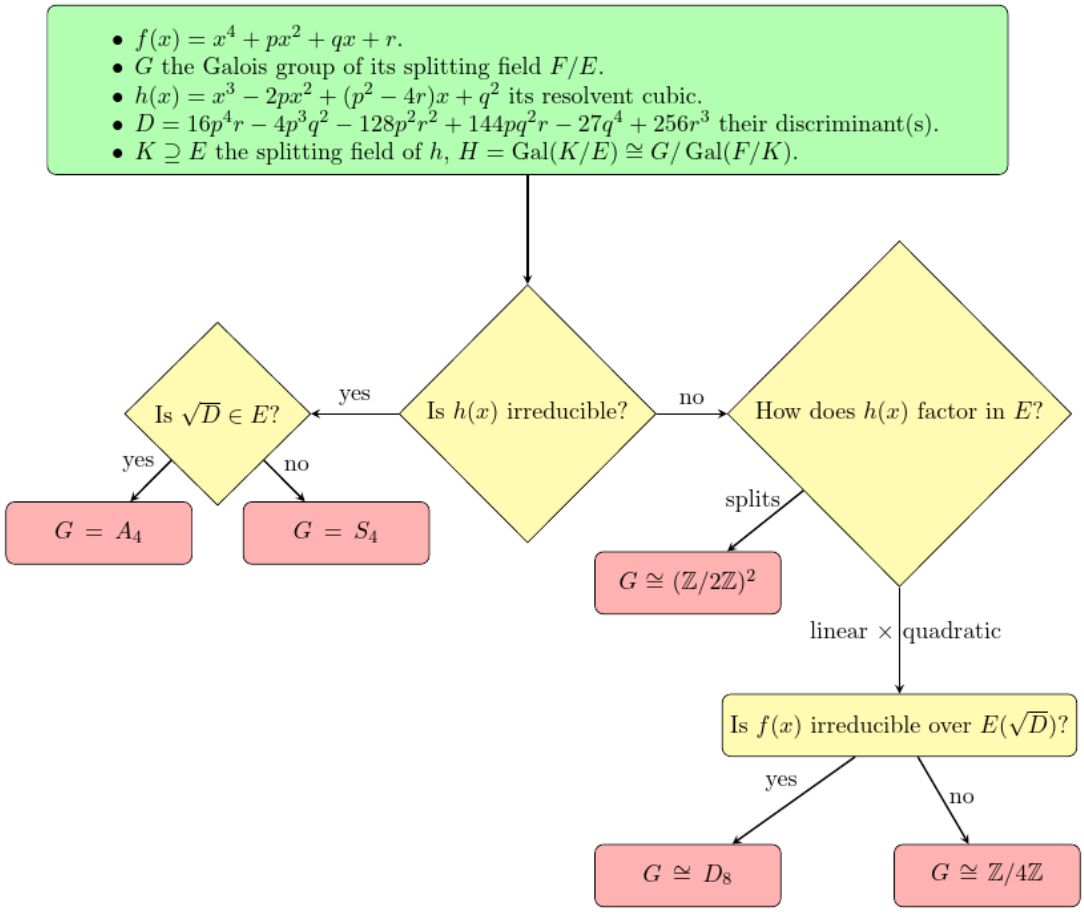
- If $\sqrt{\Delta} \in \mathbb{Q}$, then $G = A_4, C_2^2$.
  - If resolvent is irreducible: A_4. Otherwise C_2^2.
- If $\sqrt{\Delta} \notin \mathbb{Q}$ then $G = S_4, D_4, C_4$.
  - Is resolvent is irreducible: S_4. Otherwise, D_4 or C_4, argue by cycle types (or if f is irreducible in $\mathbb{Q}(\sqrt{\Delta})$, D_4).

disc f *in* K	$R_3(X)$ *in* $K[X]$	G_f
$\neq \square$	*irreducible*	S_4
$= \square$	*irreducible*	A_4
$\neq \square$	*reducible*	D_4 *or* $\mathbf{Z}/4\mathbf{Z}$
$= \square$	*reducible*	V

TABLE 4.

- Summary:

A flow chart summarizing the full process:



See Hungerford 273 for classification.

Example 9.4.16 ***(Quartics using resolvent cubics):***

- $G(x^4 - x - 1) = S_4$:
  - Check f is irreducible in $\mathbb{F}_2[x]$.

- $R_3(t) = t^4 + 4t - 1$

- $G(x^4 + 8x + 12) = A_4$:
  - The resolvent cubic is $x^3 - 48x + 64$, which has no rational roots.
  - Now check
    $$\Delta = (-27)(8^4) + (256)(12^3) = (81)(2^{12}) \in \mathbb{Q}^2,$$
    so $G = A_4$.

- $G(x^4 + 3x + 3) = D_4$:
  - The resolvent cubic is $g(x) = x^3 - 12x + 9 = (x-3)(x^2+3x-3)$ and $\Delta = 3^3 5^2 7$, so $G = C_4, D_4$.
  - Check $D \coloneqq \Delta_g = 21$.
  - Check if g is irreducible in $\mathbb{Q}(\sqrt{21})$: suppose $x^4 + 3x + 3 = \left(x^2 + ax + b\right)\left(x^2 - ax + c\right)$, then $-a^2 + b + c = 0, a(c-b) = 0, bc = 3$
    - ♢ From $a(c-b) = 0$, if $a = 0$ then $b = -c$ and $c^2 = 3$, but $\sqrt{-3} \notin \mathbb{Q}(D)$. Otherwise $c = b$ and $c^2 = 3$, but $\sqrt{3} \notin \mathbb{Q}(D)$.
  - So $G = D_4$.

9.4.4 Cyclotomic Fields

Example 9.4.17 ***(Cyclotomic Fields):*** $\mathsf{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$ 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:

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

Fact 9.4.18
The splitting field of $x^p - 1$ is $\mathbb{Q}(\zeta_p)$, and the splitting field of $x^p + 1$ is $\mathbb{Q}(\zeta_{2p})$.

- $x^p - a$ factors as $\prod_{k=0}^{p-1}(x - \zeta_p^k \omega)$ where $\omega \coloneqq a^{\frac{1}{p}}$, so this splits in $\mathbb{Q}(\zeta_p, \omega)$ which has degree
  $$\varphi(p) \cdot \deg \min_{\omega}(x) = (p-1)p.$$
  - This yields two cyclic subgroups C_{p-1}, C_p where $C_p \trianglelefteq G$, and thus some semidirect product $C_{p-1} \curvearrowright C_p$.

- $x^p + a$ factors as $\prod_{k=0}^{p-1}(x - \zeta_p^k \omega)$ for $\omega \coloneqq (-a)^{\frac{1}{p}}$.

Also use that splitting fields over $\mathbb{Q}$ are always normal, so it suffices to check that f is separable and irreducible to show extensions are Galois.

Example 9.4.19 *($x^n - a$):* Degree 3:

- $G(x^3 - 2) : S_3$
  - The roots are $\zeta_3^k \omega$ for $0 \leq k \leq 3$, $\omega \coloneqq 2^{\frac{1}{3}}$.
  - The splitting field is $\mathbb{Q}(\omega, \zeta_3)$ which has degree $3\varphi(3) = 6$.
  - The possibilities are $G = A_3 \cong C_3, S_3$, and order 6 forces $G = S_3$.
  - Useful alternative:
    - ♢ Note that there is exactly one real root and one conjugate pair, so G contains a transposition (23).
    - ♢ There is a 3-cycle (123) given by fixing ω and sending $\zeta_3 \mapsto \zeta_3 \omega$, and this is enough to generate $D_3 \cong S_3$.

Degree 4:

- $G(x^4 - 1) = C_2$:
  - The roots are ζ_4^k for $0 \leq k \leq 3$.
  - The splitting field is $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ which has degree $\varphi(4) = 2$.
  - But this is not a reducible polynomial! Use that that Galois is defined as $\mathrm{Aut}(\mathrm{SF}(f)/\mathbb{Q})$ and quadratic extensions are Galois.
- $G(x^4 - 2) = D_4$:
  - The roots are $\zeta_4^k \omega$ for $0 \leq k \leq 3$, where $\zeta_4 = i, \omega = 2^{\frac{1}{4}}$.
    - ♢ Explicitly, $r_i \in \{\omega, i\omega, -\omega, -i\omega\}$
  - The splitting field is $\mathbb{Q}(\omega, \zeta_4)$, which has degree $4\varphi(4) = 8$ since $\min_{\zeta_4} = x^2 + 1$, which is still irreducible over $\mathbb{Q}(\omega) \subseteq \mathbb{R}$.
  - $D_4 \leq S_4$ is the only transitive subgroup of order 8.
  - Useful note on bounding the size:
    - ♢ Any $\sigma \in G$ must preserves roots of $x^4 - 2$ but also $x^2 + 1$. So there are at most 4 possibilities for $\sigma(\omega)$, and at most 2 for $\sigma(\zeta_4)$, so $\#G \leq 8$ and $G \neq S_4$.
  - Explicitly, there is a 4-cycle $\sigma = (1, 2, 3, 4)$ generated by $\omega \mapsto \zeta_4 \omega$ and a 2-cycle $(2, 4)$ given by complex conjugation, and this generates D_4 since $\gcd(4 - 2, 4) \neq 1$.
    - ♢ Why this is a 4-cycle: check $\sigma(i) = i$, and:

$$\begin{aligned}
\sigma(r_1) &= r_2 = ir_1 \\
\sigma(r_2) &= \sigma(ir_1) = ir_2 = r_3 \\
\sigma(r_3) &= \sigma(ir_2) = ir_3 = i(ir_2) = -r_2 = r_4.
\end{aligned}$$

General cases:

- $G(x^p - 1) = C_p^\times$:
  - ?

Example 9.4.20 *($x^n + a$):*

- $G(x^4+1) = C_2^2$:
  - This is irreducible because it is irreducible (by having no roots) mod 3.
  - The roots are ζ_8^k for $k = 1, 3, 5, 7$ coprime to 8, since this is $\Phi_8(x)$.
  - The splitting field is $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$, noting that $\zeta_8 = e^{\frac{2\pi i}{8}} = e^{\frac{\pi i}{4}} = \cos(\pi/4) + i\sin(\pi/4) = (1/2)(\sqrt{2} + i\sqrt{2})$ so we have containment and both are degree $\varphi(8) = 4$ extensions.
  - This restricts to C_4, C_2^2.
  - Reduce mod 5 to get $(x^2+2)(x^2+2)$ of cycle type $(2,2)$, forcing C_2^2.
- $G(x^4+2) = D_4$:
  - The roots are $\zeta_8^k \omega$ for $\omega = 2^{\frac{1}{4}}, k = 1, 3, 5, 7$ coprime to 8.
  - The splitting field is $\mathbb{Q}(\zeta_8, \omega) = \mathbb{Q}(\zeta_4, \omega)$.
- $G(x^4+3) = D_4$:
  - The roots are ζ_8^k, ω for $\omega = 3^{\frac{1}{4}}, k = 1, 3, 5, 7$ coprime to 8.
  - The splitting field is $\mathbb{Q}(\omega, \zeta_8)$ of degree $\varphi(8) = 8$

9.4.5 Finite Fields

Example 9.4.21 ***(Finite Fields):*** $\mathsf{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/\langle n \rangle$, 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.

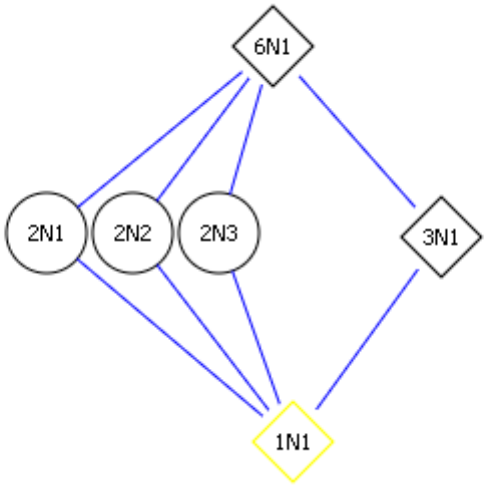
9.5 Lattices

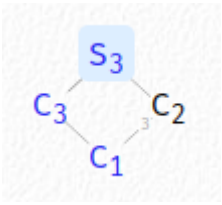
Fact 9.5.1 (Common lattices of subgroups)
$n = 2$:

- $D_2 \cong 1$
- $A_2 \cong 1$
- $S_2 \cong C_2$

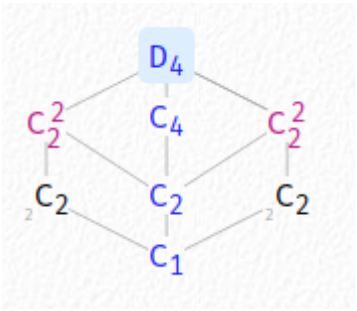
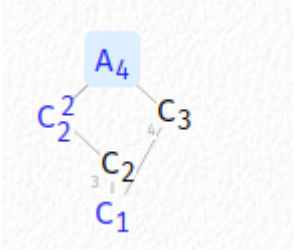
$n = 3$:

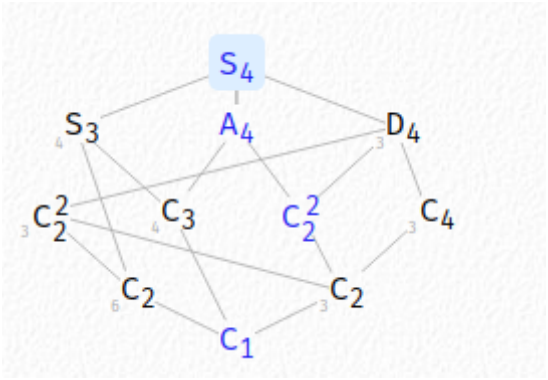
- $D_3 \cong S_3$
- $A_3 \cong C_3$.


6N1
2N1
2N2
2N3
3N1
1N1

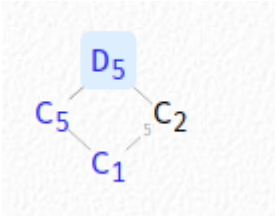
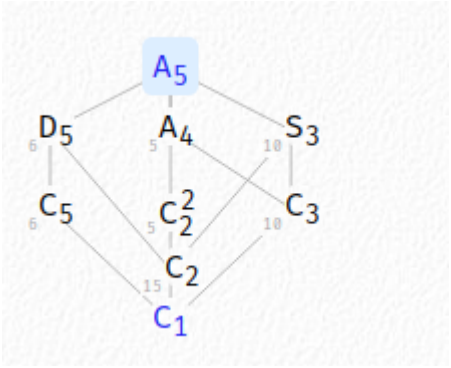
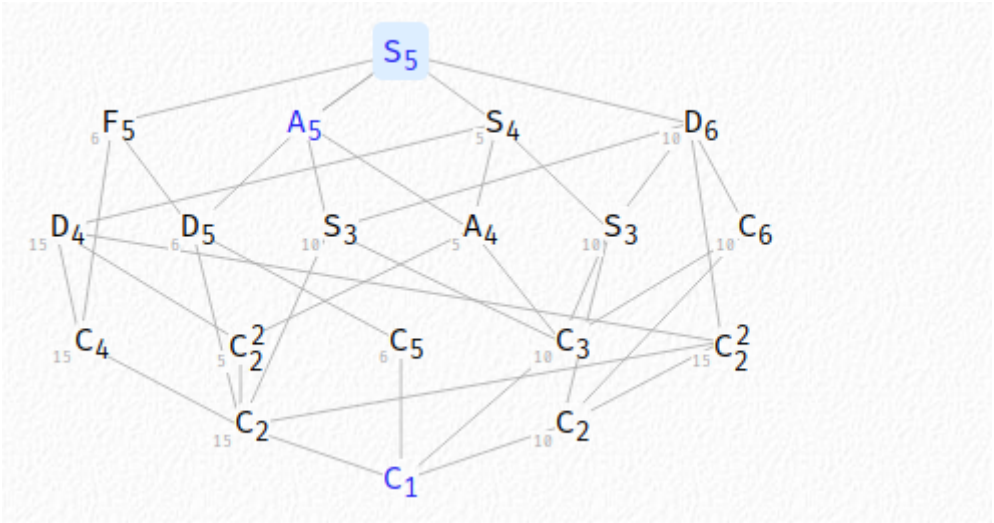
- 
S3
C3
C2
C1

$n = 4$:

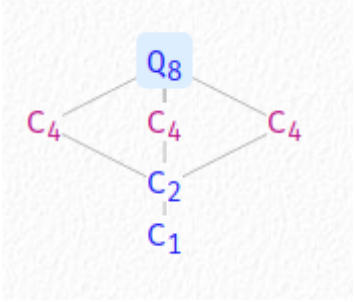
- 
D4
C4
C2
C2
C2
C2
C2
C1
- 
A4
C3
C2
C2
C1

- 
S4
S3
A4
D4
C2 2
C3
C2 2
C4
C2
C2
C1

$n = 5$:

- 
D5
C5
C2
C1
- 
A5
D5
A4
S3
C5
C2 2
C3
C2
C1
- 
S5
F5
A5
S4
D6
D4
D5
S3
A4
S3
C6
C4
C2 2
C5
C3
C2 2
C2
C2
C1

Misc:



10 Modules

10.1 Definitions and Basics

Definition 10.1.1 (R-modules)
Four properties:

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

Note that M is additionally an R-algebra if the multiplication map is R-bilinear and so given by $m : M^{\otimes_R 2} \to M$ satisfying

$$r.m(a \otimes b) = m(r.a \otimes b) = m(a \otimes r.b) \qquad \forall r \in R, a, b \in M.$$

Proposition 10.1.2 ***(The one-step submodule test).***
$N \subseteq M$ is an R-submodule iff N is nonempty and for every $r \in R$ and $x, y \in N$, we have $rx + y \in N$.

Definition 10.1.3 (Module Morphisms)
A map $f : M \to N$ is a **morphism of modules** iff $f(rm + n) = rf(m) + f(n)$.

Proposition 10.1.4 ***(One-step module morphism test).***
A map $\varphi : M \to N$ is a morphism in R-Mod iff

$$\varphi(r.x + y) = r.\varphi(x) + \varphi(y) \in N \qquad \forall r \in R, x, y \in M.$$

Remark 10.1.5: Quotients of modules are easier to reason about additively, writing $M/N = \{x + N\}$ as cosets. Then $(x + N) + (y + N) = (x + y) + N$ and $(x + N)(y + N) = (xy) + N$.

Definition 10.1.6 (Simple modules)
A module is **simple** iff it has no nontrivial proper submodules.

Definition 10.1.7 (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 10.1.8 (Cyclic modules)
A module M is **cyclic** if there exists a single generator $m \in M$ such that $M = mR \coloneqq \langle m \rangle$.

10.2 Structure Theorems

Proposition 10.2.1 ***(Isomorphism theorems).***

$$M/\ker\varphi \cong \operatorname{im}\varphi$$
$$\frac{A+B}{B} \cong \frac{A}{A\cap B}$$
$$\frac{M/A}{B/A} \cong \frac{M}{B}$$
$$\left\{\begin{smallmatrix}\text{Submodules of } M\\ \text{containing } N\end{smallmatrix}\right\} \rightleftharpoons \{\text{Submodules of } M/N\}$$
$$A \rightleftharpoons A/N.$$

Note that the lattice correspondence commutes with sums and intersections of submodules.

Proposition 10.2.2 ***(Recognizing direct sums).***
If $M_1, M_2 \leq M$ are submodules, then $M = M_1 \oplus M_2$ if the following conditions hold:

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

10.3 Exact Sequences

Definition 10.3.1 (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 $\operatorname{im} d_i = \ker d_{i+1}$.

Remark 10.3.2: Note that $C \cong B/d_1(A)$ always, but B is not a direct sum of the outer terms unless the sequence splits.

Definition 10.3.3 (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 $d_2 \circ s = \mathrm{id}_C$. ξ has a **left-splitting** iff there exists a map $t : B \to A$ such that $t \circ d_1 = \mathrm{id}_A$.

Proposition 10.3.4 ***(Equivalent conditions for splitting SESs).***
Let $\xi : 0 \to A \xrightarrow{d_1} B \xrightarrow{d_2} C \to 0$ be a SES, then TFAE

- ξ admits a right-splitting $s : C \to B$.
- C is projective.
- ξ admits a left-splitting $t : B \to A$.
- A is injective.
- ξ is isomorphic to a SES of the form $0 \to A \to A \oplus C \to C \to 0$.

Proof (?).
Right-splitting implies direct sum:

- Use that $B \subset \ker d_2 + \operatorname{im} s$, writing $b = (b - sd_2(b)) + sd_2(b)$ and noting

$$d_2(b - sd_2(b)) = d_2(b) - d_2sd_2(b) = d_2(b) - d_2(b) = 0.$$

- Show $\ker d_2 \cap \operatorname{im} s = 0$, writing b with $d_2(b) = 0$ and $b = s(c)$ for some c yields

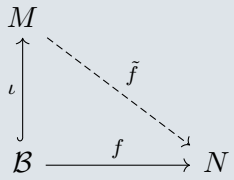
$$0 = d_2(b) = d_2s(c) = \mathrm{id}_C(c) = c.$$

■

10.4 Free and Projective Modules

Definition 10.4.1 (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:



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 $\mathcal{B} \coloneqq \{\beta_i\}_{i\in I}$,
- Direct sum decomposition:
  M decomposes as $M \cong \bigoplus_{i\in I} \beta_i R$, a sum of cyclic submodules.

Example 10.4.2 ***(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 10.4.3 (Free rank)
If a module M is free, the **free rank** of M is the cardinality of any basis.

Proposition 10.4.4 ***(?).***
Every free R-module admits a basis (spanning R-linearly independent set).

Definition 10.4.5 (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 $M_t \coloneqq \left\{m \in M \;\middle|\; \exists r \in R, rm = 0_M\right\}$ 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 10.4.6 ***(Free implies torsionfree).***
For R an integral domain, any finitely generated free R-module M is torsionfree.

Proof (that free implies torsionfree).

- If M is finitely generated, write $M = \langle X\rangle$ with $X \coloneqq \{x_1, \cdots, x_m\}$ and $\#X < \infty$ a finite generating set.
- Since M is free, there is some maximal subset of generators $\mathcal{B} \coloneqq \{x_1, \cdots, x_n\} \subseteq X$ where $n \leq m$ that is linearly independent.
- Consider $N \leq M$ defined by $\langle\mathcal{B}\rangle$; this is a basis for N and makes N free. The claim is now that $M \cong N$, so that any maximal linearly independent subset of generators is all of X.

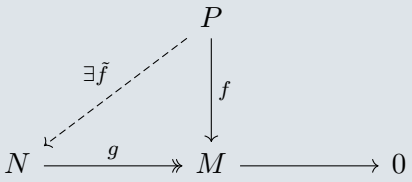
- If $N \not\cong M$, set $\mathcal{B}^c \coloneqq X \setminus \mathcal{B} = \{x_{n+1}, \cdots, x_m\}$ to be all generators for M that the basis $\mathcal{B}$ misses.
- Then $\mathcal{B}^c \cup \{x_j\}$ for any $n+1 \leq j \leq m$ has a linear dependence, and $r_j x_j + \sum_{k=1}^{n} r_n x_n = 0$ for some $r_j \neq 0$ implies $r_j x_j = -\sum_{k=1}^{n} r_n x_n$.
- Let r be the product of all of the scalars obtained this way, so $r = \prod_{k=n+1}^{m} r_j$, and consider the submodule $rX \leq N \leq M$. We get $rM \leq N \leq M$ since X is a generating set for M, so it now suffices to show $rM \cong M$.
- Just define a map $\varphi_r : M \twoheadrightarrow rM$ where $m \mapsto rm$, and note $\ker \varphi_r = \left\{ m \in M \;\middle|\; rm = 0 \right\} = 0$ since M is torsionfree. So $M = M/\ker \varphi_r \cong rM$.

■

Example 10.4.7 ***(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 $d \coloneqq \gcd(b, q)$ 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 10.4.8 (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:



Link to Diagram

- Direct summand:

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

- Splitting:

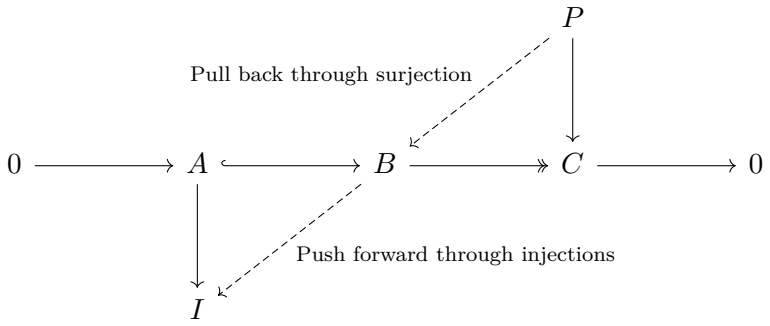
  For every SES $0 \to A \to B \to P \to 0$, there is a right section $P \to B$ such that $P \to B \to P = \mathrm{id}_P$.

  Note that this implies $B \cong \mathrm{im}(P \to B) \oplus \ker(B \to P)$.

- Exactness:

  The (always left-exact) covariant hom functor $\mathrm{Hom}(P, -)$ is right-exact.

Remark 10.4.9: There is a nice way to remember the right diagrams for injective and projective modules. The slogan is that morphisms *out* of a projective module can be *pulled* back through epimorphisms/surjections, and morphisms *into* an injective module can be *pushed* forward through monomorphisms/injections.

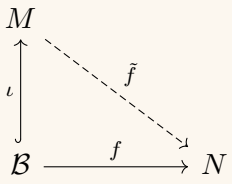


Link to Diagram

Proposition 10.4.10 ***(Free implies projective).***
Any free $M \in$ R-Mod is projective.

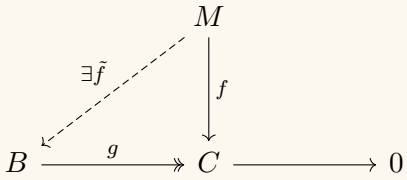
Proof (?).

- Let M be free, so that the universal property gives us this diagram:



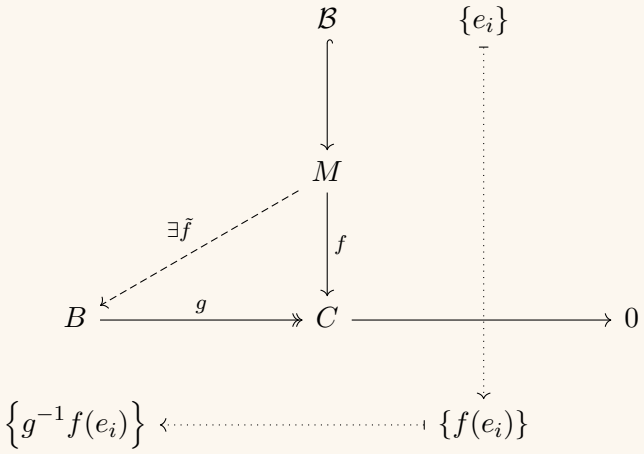
Link to Diagram

- To show M is projective, we need to produce a lift in the following diagram, where B, C are arbitrary:



Link to Diagram

- It suffices to produce a map $\mathcal{B} \to B$, since the universal property then provides $M \to B$. Here's the schematic:



Link to Diagram

- Here we write $\mathcal{B} \coloneqq \{e_i\}$, included into M, and mapped by f to C. Then use surjectivity to choose preimages in B under g arbitrarily, and this defines a morphism $\mathcal{B} \to B$.

■

Example 10.4.11 ***(Projective $\not\Longleftrightarrow$ free):*** Let R_1, R_2 be two nontrivial rings and set $R \coloneqq R_1 \oplus R_2$. Then R_1, R_2 are projective R-modules by construction, but each factor contains R-torsion: setting $e \coloneqq (0,1) \in R$ we have $e \curvearrowright R_1 = 0_{R_1}$. Since free implies torsionfree, R_1 can not be a free R-module.

10.5 Classification of Modules over a PID

Proposition 10.5.1 ***(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 10.5.2 ***(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.
$\impliedby$: Suppose $M \trianglelefteq R$ is principal, so $M = \langle \mathbf{m}\rangle$ for some $\mathbf{m} \neq \mathbf{0}_M \in M \subset R$.
Then $x \in M \implies x = \alpha\mathbf{m}$ for some element $\alpha \in R$ and we just need to show that $\alpha\mathbf{m} = \mathbf{0}_M \implies \alpha = 0_R$ in order for $\{\mathbf{m}\}$ to be a basis for M, making M a free R-module. But since $M \subset R$, we have $\alpha, m \in R$ and $\mathbf{0}_M = 0_R$, and since R is an integral domain, we have $\alpha m = 0_R \implies \alpha = 0_R$ or $m = 0_R$. Since $m \neq 0_R$, this forces $\alpha = 0_R$, which allows $\{m\}$ to be a linearly independent set and thus a basis for M as an R-module.

■

Remark 10.5.3: This says every module M decomposes as $M \cong F_M \oplus M_t$ where F_M is free (and thus torsionfree) and M_t is torsion, and moreover $F_M \cong M/M_t$.

That M/M_t is torsionfree: suppose $r(m + M_t) = M_t$, so $rm \in M_t$ is torsion. Then $r'(rm) = 0$ for some r', making m torsion, and $m + M_t = M_t$ is the zero coset.

That $F_M \cong M/M_t$: take the SES $0 \to M_t \to M \to F \to 0$ to get $F \cong M/M_t$. This splits since F is free and thus projective, so $F \cong M \oplus M_t$.

10.6 Algebraic Properties

Definition 10.6.1 (Module structure on tensor products)

$$r \curvearrowright (m \otimes n) \coloneqq (r \curvearrowright m) \otimes n.$$

Proposition 10.6.2 *(?).*

If $\dim_k V, \dim_k W < \infty$ then there is an isomorphism

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

Proposition 10.6.3 *(?).*
If either of $\dim_k V, \dim_k W$ is finite, then

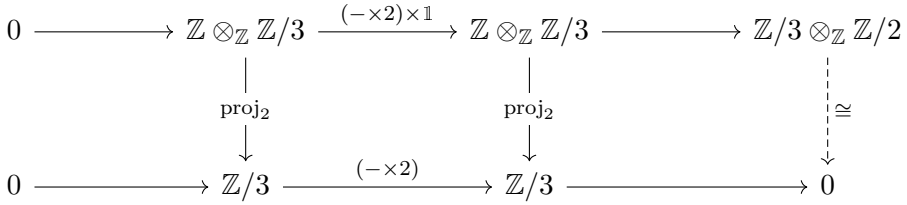
$$V^\vee \otimes_k W^\vee \xrightarrow{\sim} (V \otimes W)^\vee$$
$$v \otimes w \mapsto (x \otimes y \mapsto v(x)w(y)).$$

Proposition 10.6.4 *(?).*

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

Proposition 10.6.5 *(?).*
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 10.6.6 *(Computing tensor products):* $\mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}/3 = 0$:



Link to Diagram

11 | Linear Algebra

Remark 11.0.1: Algorithm for SNF: D&F page 479.

Remark 11.0.2: Some definitions:

- A^t is the usual transpose.
- $A^\dagger$ is the conjugate transpose.

- A matrix is $A^\dagger$ is **adjoint** to A iff $\langle A\mathbf{x},\ \mathbf{y}\rangle = \left\langle \mathbf{x},\ A^\dagger \mathbf{y}\right\rangle$.
  - A is **self-adjoint** iff A is an adjoint for itself, so $\langle A\mathbf{x},\ \mathbf{y}\rangle = \langle \mathbf{x},\ A\mathbf{y}\rangle$.
- A is **symmetric** iff $A = A^t$.
  - A is **orthogonal** iff $A^t A = AA^t = I$
- A is **Hermitian** iff $A^\dagger = A$.
  - A is **normal** iff $AA^\dagger = A^\dagger A$.
  - A is **unitary** iff $A^\dagger A = AA^\dagger = I$.

Fact 11.0.3 (Undergrad reminders)

$$\det M = \prod_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

For example,

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{array}{c} a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ -a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32} \end{array}.$$

Let $\text{minor}_A(i,j)$ denote A with the ith row, jth column deleted.

One can expand determinants along rows:

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det \text{minor}_A(i,j).$$

Also useful, a matrix can be inverted by computing the adjugate:

$$A^{-1} = \frac{1}{\det A} \operatorname{adj}(A) \qquad \operatorname{adj}(A)_{ij} \coloneqq (-1)^{i+j} \det \text{minor}_A(j,i).$$

The eigenvalues of an upper-triangular matrix are exactly the diagonal entries, and the determinant is their product. More generally, the determinant is always the product of the eigenvalues, and the trace is the sum of the eigenvalues, so $\operatorname{tr}(A) = \sum \lambda_i$ and $\det(A) = \prod \lambda_i$.

Matrices can be block-multiplied when all dimensions are compatible:

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} E & F \\ G & H \end{bmatrix} = \begin{bmatrix} AE + BG & AF + BH \\ CE + DG & CF + DH \end{bmatrix}.$$

Note that if any of these matrix multiplications don't make sense, the results won't be valid!

If A is upper triangular, some entries of A^k can be computed easily:

$$A \coloneqq \begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \implies A^k = \begin{pmatrix} a_1^k & & * \\ & \ddots & \\ 0 & & a_n^k \end{pmatrix}.$$

Traces of products can be commuted: $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, so similar matrices have identical traces since $\operatorname{tr}(PJP^{-1}) = \operatorname{tr} PP^{-1}J = \operatorname{tr} J$.

The coefficients of the characteristic polynomial are elementary symmetric functions in the eigenvalues:

$$\chi_A(t) = t^n - \left(\sum_i \lambda_i\right) t^{n-1} + \left(\sum_{i<j} \lambda_i \lambda_j\right) t^{n-2} + \cdots \pm \left(\prod_i \lambda_i\right).$$

Example 11.0.4 ***(of polynomial long division):*** Consider $f(x) \coloneqq x^3 - 6x^2 + 12x - 8$, then any rational root is in $\{\pm 8, \pm 4, \pm 2, \pm 1\}$. Testing $f(2) = 0$ works, and dividing by $x - 2$ yields

$$\begin{array}{rl}
 & x^2 \quad -4x \quad +4 \\
\hline
x-2 \quad) & x^3 \quad -6x^2 \quad +12x \quad -8 \\
 & \underline{-} \\
 & \quad x^3 \quad -2x^2 \\
 & \hline
 & \qquad\quad -4x^2 \quad +12x \quad -8 \\
 & \qquad\quad \underline{-} \\
 & \qquad\quad -4x^2 \quad +8x \\
 & \hline
 & \qquad\qquad\quad\; 4x \quad -8 \\
 & \qquad\qquad\quad\; \underline{-} \\
 & \qquad\qquad\quad\; 4x \quad -8 \\
 & \hline
 & \qquad\qquad\qquad\quad\; 0
\end{array}$$

The rest can be factored by inspection:

$$f(x) = (x-2)(x^2-4x+4) = (x-2)^3.$$

11.1 Definitions

Remark 11.1.1: 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 $p(x) \cdot \mathbf{v} \coloneqq p(T)(\mathbf{v})$. Using that $k[x]$ is a PID iff k is a field, and we can apply the FTFGMPID to get two decompositions:

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

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

- The q_i are the **invariant factors** of T
  - q_i is the minimal polynomial of T restricted to $V_i \coloneqq k[x]/\left\langle q_i(x) \right\rangle$.
  - 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 11.1.2 (Nondegenerate Bilinear Form)

todo

Definition 11.1.3 (Quadratic Form)

todo

Definition 11.1.4 (Gram Matrix)

todo

Definition 11.1.5 (Normal Matrix)
A matrix $A \in \mathrm{Mat}(n \times n; \mathbb{C})$ is **normal** iff $A^\dagger A = A A^\dagger$ where $A^\dagger$ is the conjugate transpose.

Definition 11.1.6 (Semisimple)
A matrix A over k is **semisimple** iff A is diagonalizable over k^{Alg}, the algebraic closure.

Definition 11.1.7 (Nilpotent)
A matrix A over k is **nilpotent** iff $A^k = 0$ for some $k \geq 1$.

Idea: upper triangular matrices.

Definition 11.1.8 (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 11.1.9 ***(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 11.1.10 ***(Perp of sum is intersection of perps).***

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

Definition 11.1.11 (Similar Matrices)
Two matrices A, B are **similar** (i.e. $A = PBP^{-1}$) $\iff$ A, B have the same Jordan Canonical Form (JCF).

Definition 11.1.12 (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)

11.1.1 Matrix Groups

Definition 11.1.13 (General Linear Group)

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

Proposition 11.1.14 ***(Order of*** GL_n***).***

todo

Definition 11.1.15 (Special Linear Group)

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

Definition 11.1.16 (Orthogonal Group)

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

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

Definition 11.1.17 (Special Orthogonal Group)

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

Definition 11.1.18 (Unitary Group)

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

Definition 11.1.19 (Special Unitary Group)

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

Definition 11.1.20 (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.

11.2 Minimal / Characteristic Polynomials

Proposition 11.2.1 ***(Useful computational trick).***

A trick for finding characteristic polynomials:

$$\begin{aligned}\chi_A(t) &= \sum_{k=0}^{n}(-1)^k \operatorname{tr}\left(\bigwedge^k A\right) t^{n-k} \\ &= t^n - \operatorname{tr}(A)\, t^{n-1} + \operatorname{tr}\left(\bigwedge^2 A\right) t^{n-2} - \cdots \pm \operatorname{tr}\left(\bigwedge^{n-1} A\right) t \mp \det(A),\end{aligned}$$

using that

$$\begin{aligned}\bigwedge^0 A &:= 1 \\ \bigwedge^1 A &:= A \\ \operatorname{tr}\left(\bigwedge^n A\right) &= \det(A).\end{aligned}$$

Moreover, the intermediate traces are easy to compute by hand:

$$\operatorname{tr}\left(\bigwedge^\ell A\right) = \sum \det\left(M^\ell\right),$$

where the sum is taken over all $\ell \times \ell$ **principal minors**: determinants of the $\binom{n}{\ell}$ principal matrices which are obtained by choosing ℓ diagonal entries to keep and and deleting the rows and columns for every entry not chosen. Equivalently, one can select $n - \ell$ diagonal entries and delete the corresponding row/column for each.

Example 11.2.2 *(?):*

```
sage: M
[ 0  1  2  3]
[ 4  5  6  7]
[ 8  9 10 11]
[12 13 14 15]
sage: principal_submatrices(M, 0)
[[]]
sage: principal_submatrices(M, 1)
[[0], [5], [10], [15]]
sage: principal_submatrices(M, 2)
[
[0 1]  [ 0  2]  [ 0  3]  [ 5  6]  [ 5  7]  [10 11]
[4 5], [ 8 10], [12 15], [ 9 10], [13 15], [14 15]
]
sage: principal_submatrices(M, 3)
[
[ 0  1  2]  [ 0  1  3]  [ 0  2  3]  [ 5  6  7]
[ 4  5  6]  [ 4  5  7]  [ 8 10 11]  [ 9 10 11]
[ 8  9 10], [12 13 15], [12 14 15], [13 14 15]
]
sage: principal_submatrices(M, 4)
[
[ 0  1  2  3]
[ 4  5  6  7]
[ 8  9 10 11]
[12 13 14 15]
]
sage: principal_submatrices(M, 5)
[]
```

To factor this polynomial, the **rational roots test** can be useful: for $f(t) = a_n t^n + \cdots + a_1 t + a_0$, rational roots are of the form p/q where $p \mid a_n$ and $q \mid a_0$. Note that this simplifies greatly for f monic! Once you have a root, apply **polynomial long division** to get a smaller problem, and hopefully this continues to work until it's factored.

Remark 11.2.3: 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 11.2.4 (Minimal polynomial)
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 11.2.5 (Characteristic polynomial)
The **characteristic polynomial** of A is given by

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

Fact 11.2.6
If A is upper triangular, then $\det(A) = \prod_i a_{ii}$

Theorem 11.2.7 ***(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 $\min_A(\lambda_i) = 0$.

■

11.3 Finding Minimal Polynomials

Proposition 11.3.1 ***(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 $\min_A(x) \mid p(x)$.

11.4 Other Canonical Forms

Proposition 11.4.1 ***(?).***
Let $T : V \to V$ be a linear map where $n \coloneqq \dim_k V$. 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 $1 \leq \ell \leq n$.
- $\dim_k \ker T = 1$.

11.4.1 Rational Canonical Form

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

Definition 11.4.2 (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

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

Proposition 11.4.3 ***(Equivalent conditions for cyclic vectors).***
Let V be finite dimensional and $T \in \mathrm{GL}(V)$. TFAE:

- $V \cong k[x]/\langle p \rangle$ as a $k[x]$-module.
- V admits a cyclic vector $\mathbf{v}$ where $p(x)$ is minimal degree monic polynomial such that $p(x) \curvearrowright \mathbf{v} = 0$
- V is a cyclic $k[x]$-module with annihilator ideal generated by $p(x)$.
- T is similar to the companion matrix of $p(x)$.
- $\min_T(x) = \chi_T(x)$.
- T has exactly one invariant factor.
- $\mathrm{RCF}(T)$ has a single block.

Proposition 11.4.4 ***(Minimal equals characteristic iff cyclic).***
$\chi_A(x) = \min_A(x)$ iff A admits a cyclic vector.

Proof (?).
$\not\Longleftarrow$: In general, $\min_A \mid \chi_A$, so suppose they're not equal. Set $n \coloneqq \deg \chi_A$, then if $n' \coloneqq \deg \min_A < n$, using that $\min_A(A) = 0$ this exhibits a linear dependence in $\left\{v, Av, \cdots, A^{n'}v\right\}$ for any v. In particular, since $n > n'$, any set $\{v, Av, \cdots, A^n v\}$ has a linear dependence.

$\Longrightarrow$: Apply the structure theorem to write $V \cong \bigoplus_{i=1}^{m} k[x]/\langle p_i \rangle$. Since $\chi_A(x) = \prod p_i(x)$ and $\min_A(x) = p_m(x)$, this forces $m = 1$ – one way to see this is that $\dim_k V = \sum_{i=1}^{m} \dim_k k[x]/\langle p_i \rangle$, where $\deg \chi_A = \dim_k V$ and $\deg \min_A = \dim k[x]/\langle p_m \rangle$. For these to be equal, this forces $\dim_k k[x]/\langle p_i \rangle = 0$ for $1 \leq i \leq m-1$, making V a cyclic $k[x]$-module. So $V = k[x] \curvearrowright \mathbf{v}$ for some $\mathbf{v} \in V$, which is the desired cyclic vector, and

$$V = \left\{ f(x).v \;\middle|\; f \in k[x] \right\} = \mathrm{span}_k \left\{ A^k v \;\middle|\; k \geq 0 \right\}.$$

By Cayley-Hamilton, $\chi_A(A) = 0$ and so A^n is a linear combinations of A^k for $0 \leq k \leq n-1$, so $V = \mathrm{span}_k \left\{ A^k v \;\middle|\; 0 \leq k \leq n-1 \right\}$.

■

Proposition 11.4.5 ***(Rational Canonical Form).***
$\mathrm{RCF}(A)$ is a block matrix where each block is the companion matrix of an invariant factor of

A.

Remark 11.4.6: Thus the blocks of RCF(A) biject with invariant factors of A. Note that any companion matrix is already in RCF.

Proof (Derivation of RCF).

- Let $k[x] \curvearrowright V$ by $p(x) \curvearrowright \mathbf{v} \coloneqq p(T)(\mathbf{v})$, making V into a finitely generated torsion $k[x]$-module.
  - Note that $k[x]$-submodules are exactly T-invariant subspaces.
- k a field implies $k[x]$ a PID, so apply structure theorem to obtain an invariant factor decomposition

$$V \cong k[x]/\langle \chi_T(x) \rangle \cong \bigoplus_{i=1}^{m} k[x]/\langle p_i(x) \rangle \qquad p_1(x) \mid p_2(x) \mid \cdots p_m(x).$$

- Since each factor is submodule, each corresponds to a T-invariant subspace V_i where p_i is the minimal polynomial of T restricted to V_i.
  - The largest invariant factor p_m is the minimal polynomial of T, their product is the characteristic polynomial. This follows because $p_m(x) \curvearrowright V = 0$, since $p_i \mid p_m$ for all i, forcing $\min_A \mid p_m$ by minimality.
- Write $V \cong \bigoplus_{i=1}^{m} V_i$ as a $k[x]$-module, where $V_i \coloneqq k[x]/\langle p_i(x) \rangle$, then T is a block matrix $\bigoplus_{i=1}^{m} T_i$ where T_i is the restriction of T to V_i:

$$\begin{pmatrix} T_1 & 0 & 0 & \cdots & 0 \\ 0 & T_2 & 0 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \cdots & & & T_n \end{pmatrix}.$$

- It suffices to determine the form of a single 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 with $\deg p(x) = n$.
- $\chi_M(x) = \min_M(x) \iff$ there exists a cyclic vector $\mathbf{v}$, so the set $\{\mathbf{v}_i\}_{i=0}^{n-1} \coloneqq \left\{\mathbf{v}, T\mathbf{v}, T^2\mathbf{v}, \cdots, T^{n-1}\mathbf{v}\right\}$ 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 $q(x) \coloneqq \sum_{i=1}^{n'} a_i x^i$ 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

$$p(T) = \sum_{i=1}^{n} a_i T^i \mathbf{v} = T^n + a_{n-1}T^{n-1}\mathbf{v} + a_{n-2}T^{n-2} + \cdots + a_1 T\mathbf{v} + a_0\mathbf{v} = 0,$$

  using the minimal polynomial we can write

  - $T\mathbf{v}_0 = \mathbf{v}_1$
  - $T\mathbf{v}_2 = T^2\mathbf{v}_0$
  - $T\mathbf{v}_3 = T^3\mathbf{v}_0$
  - $\cdots$
  - $T\mathbf{v}_{n-2} = T^{n-1}\mathbf{v}$
  - $T\mathbf{v}_{n-1} = T^n\mathbf{v} = -a_{n-1}T^{n-1}\mathbf{v} - \cdots - a_1 T\mathbf{v} - a_0\mathbf{v}$

- So we have

$$M_1 = \begin{bmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & 0 & & -a_2 \\ & & \ddots & 0 & \vdots \\ & & & 1 & -a_{n-1} \end{bmatrix}.$$

■

11.4.2 Smith Normal Form

Fact 11.4.7
For $A \in \mathrm{Mat}(m \times n; R)$ over R any PID, $\mathrm{SNF}(A)$ is a matrix whose diagonal entries are the invariant factors. How to compute $\mathrm{SNF}(A)$: take $A = \mathrm{diag}(a_i)$ 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 $\iff$ $\mathrm{SNF}(A) = \mathrm{SNF}(B)$.

11.4.3 Using Canonical Forms

Lemma 11.4.8 *(?).*
The characteristic polynomial is the *product of the invariant factors*, i.e.

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

Lemma 11.4.9 *(?).*

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

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

Proposition 11.4.10 ***(?).***
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

11.5 Diagonalizability

Remark 11.5.1: *Notation:* $A^\dagger$ denotes the conjugate transpose of A.

Lemma 11.5.2 ***(?).***
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 11.5.3 ***(The Spectral Theorem).***

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

Remark 11.5.4: In fact, A is symmetric $\iff$ $\operatorname{Spec} A$ forms an orthonormal basis.

Proof (of spectral theorem).

- 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 11.5.5 ***(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 11.5.6 ***(Characterizations of Diagonalizability).***
M is diagonalizable over $\mathbb{F}$ $\iff$ $\min\limits_{M}(x, \mathbb{F})$ splits into distinct linear factors over $\mathbb{F}$, or equivalently iff all of the roots of $\min\limits_{M}$ lie in $\mathbb{F}$.

Proof (?).
$\implies$: If $\min\limits_{A}$ factors into linear factors, so does each invariant factor, so every elementary divisor is linear and $JCF(A)$ is diagonal.
$\impliedby$: If A is diagonalizable, every elementary divisor is linear, so every invariant factor factors into linear pieces. But the minimal polynomial is just the largest invariant factor.

■

11.6 Matrix Counterexamples

Example 11.6.1 ***(?):*** A matrix that:

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

- $\min_M(x) = \chi_M(x) = x^2 + 1$

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

Example 11.6.2 *(?):* A matrix that:

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

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

Example 11.6.3 *(?):* Non-similar matrices with the same characteristic polynomial

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

Here $\chi_A(x) = \chi_B(x) = x^2$, but they are not conjugate since their JCFs differ (note that they're already in JCF!)

Example 11.6.4 *(?):* A full-rank matrix that is not diagonalizable:

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

Example 11.6.5 *(?):* Matrix roots of unity, i.e. representations of i:

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

11.6.1 Counting

Proposition 11.6.6 ***(Size of*** $\mathrm{GL}_n(\mathbb{F}_p)$***).***

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{n-1}).$$

It suffices to count ordered bases of $\mathbb{F}_p^n$:

- Choose $\mathbf{v}_1$: there are p choices for each coefficient, but leave out the vector 0, so $p^n - 1$ choices.
- Choose any $\mathbf{v}_2 \neq \lambda \mathbf{v}_1$, so $p^n - p$ choices.
- Choose any nonzero $\mathbf{v}_3 \neq \lambda \mathbf{v}_1 + \eta \mathbf{v}_2$, so $p^n - p^2$ choices.
- Etc.

11.7 Exercises

Exercise 11.7.1 (?)
Show that normal matrices are diagonalizable.

Exercise 11.7.2 (?)
Consider the Vandermonde matrix:

$$A \coloneqq \begin{pmatrix} 1 & \cdots & 1 \\ \lambda_1 & \cdots & \lambda_k \\ \vdots & & \vdots \\ \lambda_1^{k-1} & \cdots & \lambda_k^{k-1} \end{pmatrix}.$$

Show that

$$\det A = \prod_{i<j} (\lambda_i - \lambda_j).$$

Exercise 11.7.3 (?)
Show that a nonzero nilpotent matrix A is not diagonalizable over any field. Some useful facts:

- $\operatorname{Spec} A = \{0\}$, since $Ax = \lambda x \implies A^n = \lambda^n x$, so $A^n = 0$ forces $\lambda = 0$. This forces $\mathrm{JCF}(A)$ to be strictly upper-triangular.
- $\min_A(x) = x^n$.
- If A were diagonalizable, $\mathrm{JCF}(A) = 0$.

Exercise 11.7.4 (?)
Prove Cayley-Hamilton in the following way. Let $V = \operatorname{span}\{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$ and define the ith flag as $\mathrm{Fil}_i V \coloneqq \operatorname{span}\{\mathbf{v}_1, \cdots, \mathbf{v}_i\}$ for all $1 \leq i \leq n$, and set $\mathrm{Fil}_0 V \coloneqq \{0\}$. Show that if if A is

upper triangular, then $A(\mathrm{Fil}_i V) \subseteq \mathrm{Fil}_i V$. Now supposing $\mathbf{v}_i$ are eigenvectors for λ_i, show that

$$\begin{aligned}(A-\lambda_n I)\mathrm{Fil}_n V &\subseteq \mathrm{Fil}_{n-1} V \\ (A-\lambda_{n-1} I)(A-\lambda_n I)\mathrm{Fil}_n V &\subseteq \mathrm{Fil}_{n-2} V \\ &\vdots \\ \prod_i (A-\lambda_{n-i} I)\mathrm{Fil}_n V &\subseteq \mathrm{Fil}_0 V = \{0\}\,.\end{aligned}$$

Conclude that $\chi_A(A) = 0$.

12 | Jordan Canonical Form

Useful reference: https://mattbaker.blog/2015/07/31/the-jordan-canonical-form/

12.1 Facts

Fact 12.1.1
The JCF corresponds to **elementary divisors**.

Make more precise..

Proposition 12.1.2 ***(JCF Algorithm for generalized eigenvectors).***
The following algorithm always works for computing $\mathrm{JCF}(A)$:

- Compute and factor the characteristic polynomial as $\chi_A(x) = \prod_i (x-\lambda_i)^{m_i}$.
- For each λ_i, find the constant ℓ_i such that

$$\cdots \mathrm{rank}(A-\lambda_i I)^{\ell_i - 1} > \mathrm{rank}(A-\lambda_i I)^{\ell_i} = \mathrm{rank}(A-\lambda_i I)^{\ell_i+1} = \mathrm{rank}(A-\lambda_i I)^{\ell_i+1} = \cdots\,.$$

- Find as many usual eigenvectors $\mathbf{v}_i$ as you can. The number of eigenvectors you find will be $\dim E_{\lambda_i}$. Suppose you just get one, $\mathbf{v}$.
- Solve the systems:

$$\begin{aligned}(A-\lambda_i I)\mathbf{v}_1 = \mathbf{v} &\implies \mathbf{v}_1 = ? \\ (A-\lambda_i I)^2 \mathbf{v}_2 = \mathbf{v}_1 &\implies \mathbf{v}_2 = ? \\ &\vdots \\ &,\end{aligned}$$

which can be solved by putting the $\mathbf{v}_i$ in an augmented matrix and computing the RREF.
- This terminates in at most ℓ_i steps, and these vectors correspond to a single Jordan block.
- If there are other eigenvectors $\mathbf{w}, \cdots$ for λ_i, repeating this process yields a Jordan block for each of them. Assemble P by placing these $\mathbf{v}_i$ in the appropriate columns.

Lemma 12.1.3 ***(JCF from Minimal and Characteristic Polynomials).***
Writing $\text{Spec}(A) = \{(\lambda_i, m_i)\}$,

$$\begin{aligned} \min_A(x) &= \prod_i (x-\lambda_i)^{\ell_i} \\ \chi_A(x) &= \prod (x-\lambda_i)^{m_i} \\ E_{\lambda_i} &= \dim(A - \lambda_i I) \end{aligned}$$

- The roots both polynomials are precisely the eigenvalues λ_i of A.
  - m_i are the *algebraic multiplicities*.
  - $\dim E_{\lambda_i}$ are the *geometric multiplicities*.
- $\ell_i \leq m_i$ by Cayley-Hamilton.
- ℓ_i is
  - The size of the **largest** Jordan block associated to λ_i[a], and
  - The "stabilizing constant".
- m_i, associated to the characteristic polynomial, is
  - The **sum of sizes** of all Jordan blocks associated to λ_i,
  - The number of times λ_i appears on the diagonal of $JCF(A)$,
  - The dimension of the *generalized* eigenspace V^{λ_i}.
- $\dim E_{\lambda_i}$ is
  - The **number of Jordan blocks** associated to λ_i
  - The number of (usual) eigenvector associated to λ_i, i.e. the dimension of their span.
- A is diagonalizable iff $\dim E_{\lambda_i} = m_i$ for all i.

[a] This is because $(x-\lambda_i)^{\ell_i}$ annihilates a Jordan block of size ℓ_i, along with any blocks of size $k \leq \ell_i$.

Example 12.1.4 ***(?):*** Suppose A is 5×5 with

$$\begin{aligned} \min_A(t) &= (t-4)^2(t+6) \\ \chi_A(t) &= (t-4)^3(t+6)^2. \end{aligned}$$

Some deductions:

- For $\lambda = 4$:

  - The total size of all blocks is 3
  - The largest block is size 2
  - So this yields $J_1 \oplus J_2$.

- For $\lambda = -6$:
  - The total size of all blocks is 2
  - The largest block is size 1
  - So this must be $J_1 \oplus J_1$

⚠ Warning 12.1.5

The data of $\min_A(t), \chi_A(t)$ is **not** enough to uniquely determine JCF(A). Counterexample: there are two distinct possibilities for 4×4 matrices with $\min_A(t) = t^2$ and $\chi_A(t) = t^4$, namely $J_2 \oplus J_2$ and $J_2 \oplus J_1 \oplus J_1$.

Lemma 12.1.6 *(?).*
The elementary divisors of A are the minimal polynomials of the Jordan blocks.

Remark 12.1.7: Writing $\text{Ann}(\mathbf{v})$ as the annihilator of $\mathbf{v}$, a generalized eigenvector for the pair $(\lambda_i, \mathbf{v})$ for a matrix A is any operator in the space $\sqrt{\text{Ann}(\mathbf{v})}$, where we view V as a $k[x]$-module using $p(x) \curvearrowright \mathbf{v} \coloneqq p(A)(\mathbf{v})$. So

$$\text{Ann}(\mathbf{v}) \coloneqq \left\{ q(x) \in k[x] \;\middle|\; q(x) \curvearrowright \mathbf{v} = 0 \right\} = \left\{ q(x) \in k[x] \;\middle|\; q(A)(\mathbf{v}) = 0 \right\}.$$

Now use that $\mathbf{w}$ is an eigenvector for A with eigenvalue $\lambda_i \iff A - \lambda_i I \in \text{Ann}(\mathbf{w})$, and is a generalized eigenvector iff

$$(A - \lambda_i I)^k \in \text{Ann}(\mathbf{w}) \text{ for some } k \iff A - \lambda_i I \in \sqrt{\text{Ann}(\mathbf{w})}.$$

We can then write

$$\begin{aligned} V^{\lambda_i} &\coloneqq \left\{ \mathbf{v} \in V \;\middle|\; (A - \lambda_i I)^n \mathbf{v} = 0 \text{ for some } n \right\} \\ &= \left\{ \mathbf{v} \in V \;\middle|\; (A - \lambda_i I)^n \in \text{Ann}(\mathbf{v}) \right\} \\ &= \left\{ \mathbf{v} \in V \;\middle|\; A - \lambda_i I \in \sqrt{\text{Ann}(\mathbf{v})} \right\}, \end{aligned}$$

and the theorem is that $V \cong \bigoplus_i V^{\lambda_i}$. It also turns out that $V^{\lambda_i} = \ker(A - \lambda_i I)^n$ for $n \coloneqq \dim V$.

Proof (of generalized eigenspace decomposition).

- Suppose $\chi_A(x) = \prod (x - \lambda_i)^{n_i}$.
- Define $V^j \coloneqq \ker(A - \lambda_i I)^n$ as the generalized eigenspace for each i.
- Fix j and define $h_j(x) = \prod_{i \neq j} (x - \lambda_i)^{n_i}$, the characteristic polynomial with the λ_j term deleted.
- Define $W^j \coloneqq \text{im}(h_j(A))$, then the claim is $W^j \subseteq V^j$

  - This follows because $0 = \chi_A(A) = (A-\lambda_j I)^{n_j} h_j(A)$, so in fact $W^j \subseteq \ker(A-\lambda_j)^{n_j}$.
- Claim: $\sum V^j = V$:
  - Let $\mathbf{v} \in V$ be arbitrary, then by Euclid's algorithm write $\sum_i f_i h_i = 1$ since the h_i are coprime.
  - Thus $\sum f_i(A)h_i(A) = I \implies \left(\sum f_i(A)h_i(A)\right)(\mathbf{v}) = \mathbf{v} \implies \mathbf{v} \in \sum W^j$
- Claim: the sum is direct.
  - It suffices to show $0 = \sum w_i$ with $w_i \in W^i$ implies $w_i = 0$ for all i.
  - Use that $h_j(w_i) = 0$ for $i \neq j$ since $w_i \in W^i \coloneqq \ker(A-\lambda_I I)^{n_i}$.
  - Write $\mathbf{w}_i = \sum f_j(A)h_j(A)\mathbf{w}_i$, which collapses to $f_i(A)h_i(A)\mathbf{w}_i$.
  - So $f_i(A)h_i(A)\left(\sum w_i\right) = 0 \implies w_i = 0$.

■

Messy indexing.

12.2 Exercises

Exercise 12.2.1 (?)
Prove Cayley-Hamilton using the JCF.

Exercise 12.2.2 (?)
Prove the rank-nullity theorem using JCF.

Exercise 12.2.3 (?)
Compute JCF(A) for

$$A \coloneqq \begin{bmatrix} 1 & -1 & 0 \\ -1 & 4 & -1 \\ -4 & 13 & -3 \end{bmatrix}.$$

Solution:
- $\det(A) = 0$
- $\operatorname{tr}(A) = 2$
- $\operatorname{tr}(\bigwedge^2 A) = 1$
- $\chi_A(t) = t^3 - 2t^2 + t$
- $e_1 = [1, 1, 3]$
- $e_2 = [1, 0, -1]$
  - $e_{2,1} = [-3, -1, 0]$.

```
sage: M
[ 1 -1  0]
[-1  4 -1]
[-4 13 -3]
sage: M.characteristic_polynomial().factor()
x * (x - 1)^2
sage: M.eigenvectors_right()
[(0,
  [
  (1, 1, 3)
  ],
  1),
 (1,
  [
  (1, 0, -1)
  ],
  2)]
sage: M.jordan_form(transformation=True)
(
[0|0 0]
[-+---]  [ 1 -1  0]
[0|1 1]  [ 1  0  1]
[0|0 1], [ 3  1  3]
)
```

Exercise 12.2.4 (?)
Determine $\mathrm{JCF}(B)$ for

$$B := \begin{pmatrix} 5 & -1 & 0 & 0 \\ 9 & -1 & 0 & 0 \\ 0 & 0 & 7 & -2 \\ 0 & 0 & 12 & -3 \end{pmatrix}.$$

13 Representation Theory

Theorem 13.0.1 ***(Schur's Lemma).***
If $M \in \mathsf{G\text{-}Mod}$ is an irreducible representation of G with $\dim_k M < \infty$ and $k = \bar{k}$, then there is an isomorphism

$$M \xrightarrow{\sim} \underset{G}{\mathrm{Aut}}(M, M).$$

Theorem 13.0.2 ***(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 13.0.3 (Characters)
The **character** of a representation M is the trace of the map

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

14 | Extra Problems

14.1 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.

14.2 Group Theory

14.2.1 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.

14.2.2 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.

14.2.3 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.

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

- Show that S_n is generated by transpositions.
- Show that S_n is generated by *adjacent* transpositions.
- Show that S_n is generated by $\{(12), (12\cdots n)\}$ for $n \geq 2$
- Show that S_n is generated by $\{(12), (23\cdots n)\}$ for $n \geq 3$
- Show that S_n is generated by $\{(ab), (12\cdots n)\}$ where $1 \leq a < b \leq n$ iff $\gcd(b-a, n) = 1$.
- Show that S_p is generated by any arbitrary transposition and any arbitrary p-cycle.

14.2.5 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.

14.2.6 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.

14.2.7 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.

14.2.8 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.

14.2.9 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.

14.2.10 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

14.2.11 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.

14.2.12 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.

14.3 Ring Theory

14.3.1 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.

14.3.2 Ideals

- $\star$ Show that if x is not a unit, then x is contained in some maximal ideal.

Problem 14.3.1 (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 14.3.2 (Maximal implies prime)
Maximal $\implies$ prime, but generally not the converse.

Solution:

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

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

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

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

- Show that every proper ideal is contained in a maximal ideal
- Show that if $x \in R$ a PID, then x is irreducible $\iff \langle x \rangle \trianglelefteq R$ is maximal.
- Show that intersections, products, and sums of ideals are ideals.
- Show that the union of two ideals need not be an ideal.
- Show that every ring has a proper maximal ideal.
- Show that $I \trianglelefteq R$ is maximal iff R/I is a field.
- Show that $I \trianglelefteq R$ is prime iff R/I is an integral domain.

- Show that $\cup_{\mathfrak{m}\in \text{maxSpec}(R)} = R \setminus R^\times$.
- Show that $\text{maxSpec}(R) \subsetneq \text{Spec}(R)$ but the containment is strict.
- Show that every prime ideal is radical.
- Show that the nilradical is given by $\sqrt{0_R} = \sqrt{(0)}$.
- Show that $\text{rad}(IJ) = \text{rad}(I) \cap \text{rad}(J)$
- Show that if $\text{Spec}(R) \subseteq \text{maxSpec}(R)$ then R is a UFD.
- Show that if R is Noetherian then every ideal is finitely generated.

14.3.3 Characterizing Certain Ideals

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

$$\sqrt{0_R} \subseteq J(R).$$

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

Problem 14.3.4 (Mod by nilradical to kill nilpotents)
$R/\sqrt{0_R}$ has no nonzero nilpotent elements.

Solution:

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

Problem 14.3.5 (Nilradical is intersection of primes)
The nilradical is the intersection of all prime ideals, i.e.

$$\sqrt{0_R} = \bigcap_{\mathfrak{p}\in \text{Spec}(R)} \mathfrak{p}$$

Solution:

- $\sqrt{0_R} \subseteq \cap \mathfrak{p}$:
- $x \in \sqrt{0_R} \implies x^n = 0 \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $x^{n-1} \in \mathfrak{p}$.

- $R \setminus \sqrt{0_R} \subseteq \cup_{\mathfrak{p}}(R \setminus \mathfrak{p})$:
- Define $S = \left\{ I \trianglelefteq R \;\middle|\; a^n \notin I \text{ for any } n \right\}$.
- Then apply Zorn's lemma to get a maximal ideal $\mathfrak{m}$, and maximal $\implies$ prime.

14.3.4 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 the Jacobson radical $J(R)$.
- Show that if $R \neq 0$ is a ring in which every non-unit is nilpotent then R is local.
- Show that every prime ideal is primary.
- Show that every prime ideal is irreducible.

14.4 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.

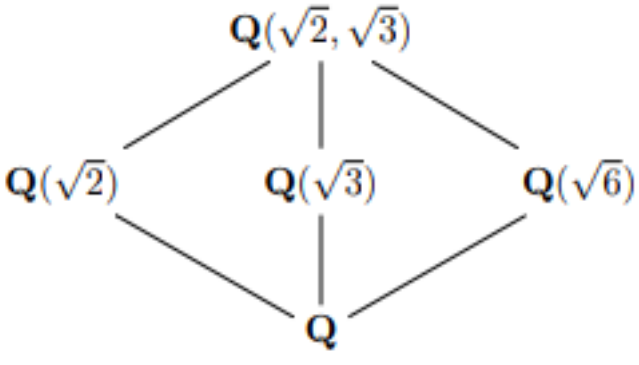
14.5 Galois Theory

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

14.5.2 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.

14.6 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 $T(\mathbf{v}_i) = \mathbf{v}_{i+1 \bmod n}$ 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.

14.7 Linear Algebra

Sort out from module section.

15 Even More Algebra Questions

Remark 15.0.1: (DZG): These all come from a random PDF I found, but I couldn't find the original author/source!

15.1 Groups

15.1.1 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?

15.1.2 Question 1.2

Prove that a subgroup of index two is normal.

15.1.3 Question 1.3

Find all normal subgroups of A_4.

15.1.4 Question 1.4

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

15.1.5 Question 1.5

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

15.1.6 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?

15.1.7 Question 1.7

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

15.1.8 Question 1.8

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

15.1.9 Question 1.9

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

15.1.10 Question 1.10

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

15.1.11 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 $p^r q^s$?

15.1.12 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.

15.1.13 Question 1.13

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

15.1.14 Question 1.14

Give examples of simple groups. Are there infinitely many?

15.1.15 Question 1.15

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

15.1.16 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.

15.1.17 Question 1.17

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

15.1.18 Question 1.18

Talk about conjugacy classes in the symmetric group S_n.

15.1.19 Question 1.19

When do conjugacy classes in S_n split in A_n?

15.1.20 Question 1.20

What is the centre of S_n? Prove it.

15.1.21 Question 1.21

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

15.1.22 Question 1.22

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

15.1.23 Question 1.23

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

15.1.24 Question 1.24

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

15.1.25 Question 1.25

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

15.1.26 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?

15.1.27 Question 1.27

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

15.1.28 Question 1.28

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

15.1.29 Question 1.29

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

15.1.30 Question 1.30

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

15.1.31 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?

15.1.32 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?

15.1.33 Question 1.33

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

15.1.34 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?

15.1.35 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?

15.1.36 Question 1.36

What groups have nontrivial automorphisms?

15.1.37 Question 1.37

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

15.1.38 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.

15.1.39 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.

15.1.40 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?

15.1.41 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.

15.1.42 Question 1.42

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

15.1.43 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?

15.1.44 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?

15.2 Classification of Finite groups

15.2.1 Question 2.1

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

15.2.2 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 $\mathbb{Q}$?

15.2.3 Question 2.3

State/prove the Sylow theorems.

15.2.4 Question 2.4

Classify groups of order 35.

15.2.5 Question 2.5

Classify groups of order 21.

15.2.6 Question 2.6

Discuss groups of order 55.

15.2.7 Question 2.7

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

15.2.8 Question 2.8

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

15.2.9 Question 2.9

Classify all groups of order 8.

15.2.10 Question 2.10

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

15.2.11 Question 2.11

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

15.2.12 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?

15.2.13 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?

15.2.14 Question 2.14

How many abelian groups are there of order 36?

15.2.15 Question 2.15

What are the abelian groups of order 16?

15.2.16 Question 2.16.

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

15.2.17 Question 2.17

How many abelian groups of order 200 are there?

15.2.18 Question 2.18

Prove there is no simple group of order 132.

15.2.19 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?

15.2.20 Question 2.20

Prove that there is no simple group of order 40.

15.3 Fields and Galois Theory

15.3.1 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.

15.3.2 Question 3.2

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

15.3.3 Question 3.3

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

15.3.4 Question 3.4

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

15.3.5 Question 3.5

What's the field with 25 elements?

15.3.6 Question 3.6

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

15.3.7 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.

15.3.8 Question 3.8

Are there separable polynomials of any degree over any field?

15.3.9 Question 3.9

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

15.3.10 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?

15.3.11 Question 3.11

What is a Galois extension?

15.3.12 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?

15.3.13 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 $\mathsf{Gal}(K/F)$ is also abelian? Give a counterexample involving number fields as well as one involving function fields.

15.3.14 Question 3.14

What is a Kummer extension?

15.3.15 Question 3.15

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

15.3.16 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?

15.3.17 Question 3.17

What is the discriminant of a polynomial?

15.3.18 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?

15.3.19 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.

15.3.20 Question 3.20

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

15.3.21 Question 3.21

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

15.3.22 Question 3.22

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

15.3.23 Question 3.23

What is the Galois group of

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

15.3.24 Question 3.24

What is the Galois group of

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

15.3.25 Question 3.25

What are the Galois groups of irreducible cubics?

15.3.26 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?

15.3.27 Question 3.27

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

15.3.28 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?

15.3.29 Question 3.29

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

15.3.30 Question 3.30

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

15.3.31 Question 3.31

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

15.3.32 Question 3.32

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

15.3.33 Question 3.33

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

15.3.34 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.

15.3.35 Question 3.35

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

15.3.36 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?

15.3.37 Question 3.37

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

15.3.38 Question 3.38

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

15.3.39 Question 3.39

Describe the Galois theory of cyclotomic extensions.

15.3.40 Question 3.40

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

15.3.41 Question 3.41

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

15.3.42 Question 3.42

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

15.3.43 Question 3.43

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

15.3.44 Question 3.44

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

15.3.45 Question 3.45

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

15.3.46 Question 3.46

Give a polynomial with S_3 as its Galois group.

15.3.47 Question 3.47

Give an example of a cubic with Galois group S_3.

15.3.48 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.

15.3.49 Question 3.49

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

15.3.50 Question 3.50

Which finite groups are Galois groups for some field extension?

15.3.51 Question 3.51

What Galois group would you expect a cubic to have?

15.3.52 Question 3.52

Draw the subgroup lattice for S_3.

15.3.53 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?

15.3.54 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 $\mathsf{Gal}(K/Q) = S_n$. What can you say about the roots?

15.3.55 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?

15.3.56 Question 3.56.

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

15.3.57 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 $1 \bmod m$.

15.3.58 Question 3.58

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

15.3.59 Question 3.59

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

15.3.60 Question 3.60

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

15.3.61 Question 3.61

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

15.3.62 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.

15.3.63 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?

15.3.64 Question 3.64

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

15.3.65 Question 3.65

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

15.3.66 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?

15.3.67 Question 3.67

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

15.3.68 Question 3.68

State and prove Eisenstein's Criterion.

15.3.69 Question 3.69

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

15.3.70 Question 3.70

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

15.3.71 Question 3.71

What are the symmetric polynomials?

15.3.72 Question 3.72

State the fundamental theorem of symmetric polynomials.

15.3.73 Question 3.73

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

15.3.74 Question 3.74

Find a non-symmetric polynomial whose square is symmetric.

15.3.75 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?

15.3.76 Question 3.76

Define p-adic numbers. What is a valuation?

15.3.77 Question 3.77

What's Hilbert's theorem 90?

15.3.78 Question 3.78

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

15.4 Normal Forms

15.4.1 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?

15.4.2 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.

15.4.3 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?

15.4.4 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?

15.4.5 Question 4.5

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

15.4.6 Question 4.6

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

15.4.7 Question 4.7

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

15.4.8 Question 4.8

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

15.4.9 Question 4.9

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

15.4.10 Question 4.10

What is rational canonical form?

15.4.11 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.

15.4.12 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.

15.4.13 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?

15.4.14 Question 4.14

What is a nilpotent matrix?

15.4.15 Question 4.15

When do the powers of a matrix tend to zero?

15.4.16 Question 4.16

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

15.4.17 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.

15.4.18 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 $SL_n(R)$?

15.4.19 Question 4.19

Is a square matrix always similar to its transpose?

15.4.20 Question 4.20

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

15.4.21 Question 4.21

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

15.5 Matrices and Linear Algebra

15.5.1 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?

15.5.2 Question 5.2

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

15.5.3 Question 5.3

Explain geometrically how you diagonalise a quadratic form.

15.5.4 Question 5.4

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

15.5.5 Question 5.5

Classify real division algebras.

15.5.6 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?

15.5.7 Question 5.7

Do you know about singular value decomposition?

15.5.8 Question 5.8

What are the eigenvalues of a symmetric matrix?

15.5.9 Question 5.9

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

15.5.10 Question 5.10

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

15.5.11 Question 5.11

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

15.5.12 Question 5.12

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

15.5.13 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.

15.5.14 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.

15.5.15 Question 5.15

State/prove the Cayley–Hamilton theorem.

15.5.16 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?

15.5.17 Question 5.17

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

15.5.18 Question 5.18

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

15.5.19 Question 5.19

What is a Toeplitz operator?

15.5.20 Question 5.20

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

15.6 Rings

15.6.1 Question 6.1

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

15.6.2 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?

15.6.3 Question 6.3

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

15.6.4 Question 6.4

Do polynomials in several variables form a PID?

15.6.5 Question 6.5

Prove that the integers form a PID.

15.6.6 Question 6.6

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

15.6.7 Question 6.7

What is the relation between Euclidean domains and PIDs?

15.6.8 Question 6.8

Do you know a PID that's not Euclidean?

15.6.9 Question 6.9

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

15.6.10 Question 6.10

Is a ring of formal power series a UFD?

15.6.11 Question 6.11

Is a polynomial ring over a UFD again a UFD?

15.6.12 Question 6.12

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

15.6.13 Question 6.13

Give an example of a ring where unique factorisation fails.

15.6.14 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.

15.6.15 Question 6.15

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

15.6.16 Question 6.16

Find all primes in the ring of Gaussian integers.

15.6.17 Question 6.17

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

15.6.18 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?

15.6.19 Question 6.19

Do you know about Dedekind domains and class numbers?

15.6.20 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?

15.6.21 Question 6.21

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

15.6.22 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 $\sqrt{I}$.

15.6.23 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.

15.6.24 Question 6.24

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

15.6.25 Question 6.25

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

15.6.26 Question 6.26

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

15.6.27 Question 6.27

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

15.6.28 Question 6.28

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

15.6.29 Question 6.29

Is the following map an isomorphism?

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

15.6.30 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.

15.6.31 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?

15.6.32 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?

15.6.33 Question 6.33

Define "Noetherian ring". give an example.

15.6.34 Question 6.34

Prove the Hilbert basis theorem.

15.6.35 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?

15.6.36 Question 6.36

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

15.6.37 Question 6.37

Give an example of an Artinian ring.

15.6.38 Question 6.38

State the structure theorem for semisimple Artinian rings.

15.6.39 Question 6.39

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

15.6.40 Question 6.40

What is a matrix algebra?

15.6.41 Question 6.41

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

15.6.42 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?

15.6.43 Question 6.43

State the structure theorem for simple rings.

15.6.44 Question 6.44

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

15.6.45 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:

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

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

15.6.46 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.

15.6.47 Question 6.47

Prove that all finite integral domains are fields.

15.6.48 Question 6.48

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

15.6.49 Question 6.49

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

15.6.50 Question 6.50

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

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

15.6.52 Question 6.52

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

15.7 Modules

15.7.1 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?

15.7.2 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?

15.7.3 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?

15.7.4 Question 7.4

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

15.7.5 Question 7.5

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

15.7.6 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?

15.7.7 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?

15.7.8 Question 7.8

What is a projective module?

15.7.9 Question 7.9

What is an injective module?

15.7.10 Question 7.10

Do you know an example of a flat module?

15.8 Representation Theory

15.8.1 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.

15.8.2 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?

15.8.3 Question 8.3

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

15.8.4 Question 8.4

State/prove/explain Schur's lemma.

15.8.5 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?

15.8.6 Question 8.6

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

15.8.7 Question 8.7

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

15.8.8 Question 8.8

Why is the character table a square?

15.8.9 Question 8.9

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

15.8.10 Question 8.10

What's the regular representation?

15.8.11 Question 8.11

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

15.8.12 Question 8.12

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

15.8.13 Question 8.13

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

15.8.14 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?

15.8.15 Question 8.15

What is Frobenius reciprocity?

15.8.16 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?

15.8.17 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?

15.8.18 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?

15.8.19 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?

15.8.20 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.

15.8.21 Question 8.21

What are the irreducible representations of finite abelian groups?

15.8.22 Question 8.22

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

15.8.23 Question 8.23

Are there two nonisomorphic groups with the same representations?

15.8.24 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?

15.8.25 Question 8.25

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

15.8.26 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?

15.8.27 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?

15.8.28 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.

15.8.29 Question 8.29

Write the character table for S_4.

15.8.30 Question 8.30

Start constructing the character table for S_5.

15.8.31 Question 8.31.

How many irreducible representations does S_n have?

What classical function in mathematics does this number relate to?

15.8.32 Question 8.32

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

15.8.33 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?

15.8.34 Question 8.34

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

15.8.35 Question 8.35

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

15.8.36 Question 8.36

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

15.8.37 Question 8.37

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

15.9 Categories and Functors

15.9.1 Question 9.1

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

15.9.2 Question 9.2

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

15.9.3 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 $\mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})$?

16 Appendix: Extra Topics

Proposition 16.0.1 ***(NC Theorem).***
$N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Definition 16.0.2 (Normalizers Grow)
If for every proper $H < G$, $H \trianglelefteq N_G(H)$ is again proper, then "normalizers grow" in G.

16.1 Characteristic Subgroups

Slogan 16.1.1
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 16.1.2 (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 16.1.3 ***(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 16.1.4 ***(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 16.1.5 ***(Centers are characteristic).***
For any group G,

$$Z(G) \operatorname{ch} G.$$

Proof (?).
Let $\psi \in \operatorname{Aut}(H)$ and $x = \psi(y) \in \psi(Z(H))$ so $y \in Z(H)$, then for arbitrary $h \in H$,

$$\begin{aligned} \psi(y)h &= \psi(y)(\psi \circ \psi^{-1})(h) \\ &= \psi(y \cdot \psi^{-1}(h)) \\ &= \psi(\psi^{-1}(h) \cdot y) && \text{since } \psi^{-1}(h) \in H,\ y \in Z(H) \\ &= h\psi(y). \end{aligned}$$

■

16.2 Normal Closures and Cores

Definition 16.2.1 (Normal Closure of a Subgroup)
The smallest normal subgroup of G containing H:

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

Definition 16.2.2 (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 16.2.3 ***(Fratini's Argument).***
If $H \trianglelefteq G$ and $P \in \mathrm{Syl}_p(G)$, then $HN_G(P) = G$ and $[G : H]$ divides $|N_G(P)|$.

16.2.1 Exercises

Exercise 16.2.4 (?)
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 $Z(G) \subseteq \psi(Z(G))$.

16.3 Nilpotent Groups

Definition 16.3.1 (Nilpotent)
A group G is **nilpotent** iff G has a terminating upper central series.

Moral: the adjoint map is nilpotent.

Theorem 16.3.2 ***(Characterization of Nilpotent Groups).***
G is nilpotent iff G has an upper central series terminating at G.

Theorem 16.3.3 *(Characterization of Nilpotent Groups).*
G is nilpotent iff G has a lower central series terminating at 1.

Theorem 16.3.4 *(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 16.3.5 *(Nilpotent Implies Maximal Normals).*
A group G is nilpotent iff every maximal subgroup is normal.

Proposition 16.3.6.
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 16.3.7

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

Todo. Speci

16.4 Rings

Definition 16.4.1 (Gorenstein Rings)
A commutative Noetherian ring R is **Gorenstein** iff R viewed as an R-module has finite injective dimension.

Example 16.4.2 *(Why care about Gorenstein rings?):* If $R \in \mathsf{gr}\,\mathsf{Alg}_{/k}$ with $\dim_k R < \infty$, then R decomposes as $R = R_0 \oplus R_1 \oplus \cdots R_n$ with $R_0 \coloneqq k$, and R is Gorenstein iff R satisfies "Poincaré duality": $\dim_k R_0 = \dim_k R_m = 1$ and there is a perfect pairing $R_i \otimes_k R_{n-j} \to R_n$.

17 | UGA Fall 2019 Problem Sets

17.1 Problem Set One

17.1.1 Exercises

Problem 17.1.1 (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 17.1.2 (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 17.1.3 (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 17.1.4 (Hungerford 2.2.12.b.)
Determine (up to isomorphism) all abelian groups of order 64; do the same for order 96.

Problem 17.1.5 (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 17.1.6 (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 17.1.7 (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 17.1.8 (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.

17.1.2 Qual Problems

Problem 17.1.9
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

$$\forall P \in X_p, \exists g \in G, P' \in X_p \;\Big|\; gP'g^{-1} = P.$$

   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

$$\begin{aligned} \ker\varphi &= \{g \in G \;\Big|\; \gamma_g = \mathrm{id}_{X_p}\} \\ &= \{g \in G \;\Big|\; \forall P \in X_p,\ gPg^{-1} = P\} \\ &= \bigcap_{P \in X_p} N_G(P), \end{aligned}$$

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 $n_p = 1 \bmod p$ 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 $n_p = 1 \bmod p$ 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 $n_3 = 1 \bmod 3$ 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 $n_3 = 1 \bmod 3$ and n_3 divides 4, which forces $n_3 = 1$ and thus G can't be simple.

   If $ap^k = 3(2^k)$, then $n_2 = 1 \bmod 2$ 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 17.1.10
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 $l \mid m$.

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 $P_N \in \text{Syl}(p, G/N)$. By the subgroup correspondence theorem, $P_n = H/N$ for some $H \leq G$ such that $N \subseteq H$.

   So choose $P_H \in \text{Syl}(p, H)$; the claim is that $P_H \in \text{Syl}(p, G)$ 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 $P_H \in \text{Syl}(p, G)$, 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 $P_H N/N \in \text{Syl}(p, G/N)$. 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 $P_H N/N \in \text{Syl}(p, G/N)$.

   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 17.1.11
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

$$C_H = \{gHg^{-1} \;\middle|\; g \in G\}$$

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.

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

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

$$K \coloneqq \{g_i H g_i^{-1} \;\middle|\; 1 \leq i \leq k\}.$$

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

$$\begin{aligned} g_i H g_i^{-1} &= g_j H g_j^{-1} \implies \\ g_j^{-1} g_i H g_i^{-1} g_j &= H \implies \\ (g_j^{-1} g_i) H (g_j^{-1} g_i)^{-1} &= H \implies \\ g_j^{-1} g_i &\in N_G(H) \implies \\ g_i &\in g_j N_G(H) \implies \\ g_i &= g_j, \end{aligned}$$

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 17.1.12
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.

5	$(1\ 2\ 3\ 4\ 5)$
$4+1$	$(1\ 2\ 3\ 4)(5)$
$3+2$	$(1\ 2\ 3)(4\ 5)$
$3+1+1$	$(1\ 2\ 3)(4)(5)$
$2+2+1$	$(1\ 2)(3\ 4)(5)$
$2+1+1+1$	$(1\ 2)(3)(4)(5)$
$1+1+1+1+1$	$(1)(2)(3)(4)(5)$

17.2 Problem Set Two

17.2.1 Exercises

Problem 17.2.1 (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 17.2.2 (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 17.2.3 (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 17.2.4 (Hungerford 2.6.4)
What is the center of the quaternion group Q_8? Show that $Q_8/Z(Q_8)$ is abelian.

Problem 17.2.5 (Hungerford 2.6.9)
Classify up to isomorphism all groups of order 18. Do the same for orders 20 and 30.

Problem 17.2.6 (Hungerford 1.9.1)
Show that every non-identity element in a free group F has infinite order.

Problem 17.2.7 (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 $\{x^n \mid x \in F\}$. Show that $H_n \trianglelefteq F$.

17.2.2 Qual Problems

Problem 17.2.8
List all groups of order 14 up to isomorphism.

Problem 17.2.9
Let G be a group of order p^3 for some prime p. Show that either G is abelian, or $|Z(G)| = p$.

Problem 17.2.10
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 17.2.11
Show that S_4 is a solvable, nonabelian group.

17.3 Problem Set Three

17.3.1 Exercises

Problem 17.3.1 (Hungerford 2.7.10)
Show that S_n is solvable for$n \leq 4$ but S_3 and S_4 are not nilpotent.

Problem 17.3.2 (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 17.3.3 (Hungerford 2.8.9)
Show that any group of order p^2q(for primes p, q) is solvable.

Problem 17.3.4 (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 17.3.5 (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 17.3.6 (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 17.3.7 (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.

17.3.2 Qual Problems

Problem 17.3.8
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 17.3.9
Determine for which integers the ring $\mathbb{Z}/n\mathbb{Z}$ is a direct sum of fields. Carefully prove your answer.

Problem 17.3.10
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 17.3.11

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.

17.4 Problem Set Four

17.4.1 Exercises

Problem 17.4.1 (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 17.4.2 (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 17.4.3 (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 $c^p \equiv c \bmod p$ for all $c \in \mathbb{Z}$.

Problem 17.4.4 (Hungerford 5.5.3)
Show that if $|K| = p^n$, then every element of K has a unique pth root in K.

Problem 17.4.5 (Hungerford 5.5.10)
Show that every element in a finite field can be written as the sum of two squares.

Problem 17.4.6 (Hungerford 5.6.1)
Let F/K be a field extension. Let $\text{char}K = p \neq 0$ 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 17.4.7 (Hungerford 5.6.8)
If $\text{char}K = p \neq 0$ and $[F : K]$ is finite and not divisible by p, then F is separable over K.

17.4.2 Qual Problems

Problem 17.4.8
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 17.4.9
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 17.4.10
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.

17.5 Problem Set Five

17.5.1 Exercises

Problem 17.5.1 (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 17.5.2 (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 17.5.3 (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 17.5.4 (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 17.5.5 (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 17.5.6 (Hungerford 5.6.11)
If $f \in K[x]$ is irreducible of degree $m > 0$ and $\text{char}(K)$ does not divide m, then f is separable.

17.5.2 Qual Problems

Problem 17.5.7
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 $\text{Gal}(E/K) \trianglelefteq \text{Gal}(E/F)$.

Problem 17.5.8
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 17.5.9
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 $M/\mathbb{F}_{13}$?

17.6 Problem Set Six

17.6.1 Exercises

Problem 17.6.1 (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 17.6.2 (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 17.6.3 (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 17.6.4 (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 17.6.5 (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 17.6.6 (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 $K \subset K(u) \subset E$.

17.6.2 Qual Problems

Problem 17.6.7

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 17.6.8
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 17.6.9
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.

17.7 Problem Set Seven

17.7.1 Exercises

Problem 17.7.1 (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 17.7.2 (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 17.7.3 (Hungerford 4.1.7)

1. Show that if A, B are R-modules, then the set $\mathrm{Hom}_R(A, B)$ 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 $\mathrm{Hom}_R(A, A)$ is a ring with identity, where multiplication is given by composition of functions.

   Note that $\mathrm{Hom}_R(A, A)$ *is called the* ***endomorphism ring*** *of* A.
3. Show that A is a left $\mathrm{Hom}_R(A, A)$-module with an action defined by

   $$a \in A, f \in \mathrm{Hom}_R(A, A) \implies f \curvearrowright a \coloneqq f(a).$$

Problem 17.7.4 (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 17.7.5 (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

$$pA \coloneqq \{pa \;\middle|\; a \in A\}$$

$$A[p] \coloneqq \{a \in A \;\middle|\; pa = 0\}.$$

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 17.7.6 (Hungerford 4.2.8)
If V is a finite dimensional vector space and

$$V^m \coloneqq V \oplus V \oplus \cdots \oplus V \quad (m \text{ summands}),$$

then for each $m \geq 1$, V^m is finite dimensional and $\dim V^m = m(\dim V)$.

Problem 17.7.7 (Hungerford 4.2.9)
If F_1, F_2 are free modules of a ring with the invariant dimension property, then

$$\text{rank}(F_1 \oplus F_2) = \text{rank}F_1 + \text{rank}F_2.$$

17.7.2 Qual Problems

Problem 17.7.8
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 17.7.9
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

$$\text{Ann}(\mu) = \{r \in R \,\big|\, r\mu = 0\}.$$

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 $I = \text{Ann}(\mu)$.
Prove that I is a *prime* ideal in R.

Problem 17.7.10
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 $I = Ra$.

17.8 Problem Set Eight

17.8.1 Exercises

Problem 17.8.1 (Hungerford 4.4.1)
Show the following:

1. For any abelian group A and any positive integer m,
$$\mathrm{Hom}(\mathbb{Z}_m, A) \cong A[m] \coloneqq \{a \in A \mid ma = 0\}.$$
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 17.8.2 (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 17.8.3 (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 17.8.4 (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 $A^{**} \coloneqq \mathrm{Hom}_R(\mathrm{Hom}(A, R), R)$ by the map
$$\overline{f} : \mathrm{Hom}(B, R) \to \mathrm{Hom}_R(A, R).$$

Problem 17.8.5 (Hungerford 4.6.2)
Show that every free module over a unital integral domain is torsion-free. Show that the converse is false.

Problem 17.8.6 (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 17.8.7 (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 $\operatorname{lcm}(r, s)$.

17.8.2 Qual Problems

Problem 17.8.8
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 $M \coloneqq R^n/\operatorname{im}(A)$.

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 $R \coloneqq F[x]$. Give an example of an integer $n > 0$ and an $n \times n$ square matrix $A \in M_n(R)$ such that $M \coloneqq R^n/\operatorname{im}(A)$ is isomorphic as an $R-$module to $R \times F$.

Problem 17.8.9

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 17.8.10
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.

17.9 Problem Set Nine

17.9.1 Exercises

Problem 17.9.1 (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 17.9.2 (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 17.9.3 (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 17.9.4 (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 $BA = I_m$) $\iff$ rank$A = m$. Similarly, show A has a right $m \times n$ inverse $\iff$ rank$A = n$.

Problem 17.9.5 (Hungerford 7.2.4)

1. Show that a system of linear equations

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m &= b_1 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m &= b_n \end{aligned}$$

   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 17.9.6 (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 $d_i \mid d_{i+1}$.
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.

17.9.2 Qual Problems

Problem 17.9.7
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 17.9.8
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 17.9.9
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.

17.10 Problem Set Ten

17.10.1 Exercises

Problem 17.10.1 (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 17.10.2 (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 17.10.3 (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 17.10.4 (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 17.10.5 (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 17.10.6 (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

$$\psi(u) = xu - \varphi(u) = \varphi(u) - \varphi(u) = 0 \qquad \forall u \in E.$$

Problem 17.10.7 (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.

17.10.2 Qual Problems

Problem 17.10.8
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 17.10.9
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 17.10.10
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.