UGA Algebra Qualifying Exam Solutions (Spring 2011 – Spring 2021)

Table of Contents

Contents

1 Preface

I'd like to extend my gratitude to the following people for helping supply solutions and proofs:

- Paco Adajar
- Swaroop Hegde

Many other solutions contain input and ideas from other graduate students and faculty members at UGA, along with questions and answers posted on Math Stack Exchange or Math Overflow.

2 Group Theory: General

2.1 Cosets

2.1.1 Spring 2020 #2 ✨

Let H be a normal subgroup of a finite group G where the order of H and the index of H in G are relatively prime. Prove that no other subgroup of G has the same order as H.

Concepts Used:

- Division algorithm: $(a, b) = d \implies as + bt = 1$ for some s, t.
- Coset containment trick: $X \subseteq N \iff xN = N$ for all x.

Strategy:
Recognize that it suffices to show $hN = N$. Context cue: coprimality hints at division algorithm. Descend to quotient so you can leverage both the order of h *and* the order of cosets simultaneously.

Solution:

- For ease of notation, replace H in the problem with N so we remember which one is normal.
- Write $n := \#N$ and $m := [G : N] = \#G/N$, where the quotient makes sense since N is normal.
- Let $H \leq G$ with $\#H = n$, we'll show $H = N$.
  - Since $\#H = \#N$ it suffices to show $H \subseteq N$.
  - It further suffices to show $hN = N$ for all $h \in H$.
- Noting $\gcd(m, n) = 1$, use the division algorithm to write $1 = ns + mt$ for some $s, t \in \mathbb{Z}$.

- The result follows from a computation:

$$\begin{aligned} hN &= h^1 N \\ &= h^{ns+mt} N \\ &= h^{ns} N \cdot h^{mt} N \\ &= (h^n N)^s \cdot \left(h^t N\right)^m \\ &= (eN)^s \cdot N \\ &= N, \end{aligned}$$

  - We've used that $h \in H \implies o(h) \mid \#H = n$ by Lagrange, so $h^n = e$.
  - We've also used that $\#G/N = m$, so $(xH)^m = H$ for any $xH \in G/H$.

2.1.2 Fall 2014 #6 ✨

Let G be a group and $H, K < G$ be subgroups of finite index. Show that

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

Concepts Used:

- For $H, K \leq G$, intersection is again a subgroup of everything: $H \cap K \leq H, K, G$ by the one-step subgroup test.
- Counting in towers: $A \leq B \leq C \implies [C : A] = [C : B][B : A]$.
- Fundamental theorem of cosets: $xH = yH \iff xy^{-1} \in H$.
- Common trick: just list out all of the darn cosets!

Strategy:
Count in towers, show that distinct coset reps stay distinct.

Solution:

- $H \cap K \leq H \leq G \implies [G : H \cap K] = [G : H][H : H \cap K]$
- So it suffices to show $[H : H \cap K] \leq [G : K]$
- Write $H/H \cap K = \{h_1 J, \cdots, h_m J\}$ as distinct cosets where $J := H \cap J$.
- Then $h_i J \neq h_j J \iff h_i h_j^{-1} \notin J = H \cap K$.
- H is a subgroup, so $h_i h_j^{-1} \in H$ forces this not to be in K.
- But then $h_i K \neq h_j K$, so these are distinct cosets in G/K.
- So $\#G/K \geq m$.

2.1.3 Spring 2013 #3 ✨

Let P be a finite p-group. Prove that every nontrivial normal subgroup of P intersects the center of P nontrivially.

Clean up, sketchy argument.

Solution:

- Let $N \trianglelefteq P$, then for each conjugacy class $[n_i]$ in N, $H \cap [g_i] = [g_i]$ or is empty.
- $G = \coprod_{i \leq M} [g_i]$ is a disjoint union of conjugacy classes, and the conjugacy classes of H are of the form $[g_i] \cap H$.
- Then pull out the center

$$H = \coprod_{i \leq M} [g_i] \cap H = (Z(G) \cap H) \coprod \coprod_{i \leq M'} [g_i].$$

- Taking cardinalities,

$$\#H = \#\left(Z(G) \cap H\right) + \sum_{i \leq M'} \#[g_i].$$

- p divides H since $H \leq P$ and P is a p-group.
- Each $\#[g_i] \geq 2$ since the trivial conjugacy classes appear in the center, forcing $\#[g_i] \geq p$.
- p divides $\#[g_i]$ since $\#[g_i]$ must divide $\#P = p^k$
- So p must divide the remaining term $Z(G) \cap H$, which makes it nontrivial.

2.2 Burnside / Class Equation

2.2.1 Spring 2019 #4 ✨

For a finite group G, let $c(G)$ denote the number of conjugacy classes of G.

a. Prove that if two elements of G are chosen uniformly at random,then the probability they commute is precisely

$$\frac{c(G)}{|G|}.$$

b. State the class equation for a finite group.

c. Using the class equation (or otherwise) show that the probability in part (a) is at most

$$\frac{1}{2} + \frac{1}{2[G : Z(G)]}.$$

Here, as usual, $Z(G)$ denotes the center of G.

⚠ Warning 2.2.1

(DZG) This is a slightly anomalous problem! It's fun and worth doing, because it uses the major counting formulas. Just note that the techniques used in this problem perhaps don't show up in other group theory problems.

Concepts Used:

- Notation: X/G is the set of G-orbits
- Notation: $X^g = \left\{x \in X \mathrel{\Big|} g \cdot x = x\right\}$
- Burnside's formula: $\#X/G = \frac{1}{\#G} \sum \#X^g$.
- Definition of conjugacy class: $C(g) = \left\{hgh^{-1} \mathrel{\Big|} h \in G\right\}$.

Strategy:

Fixed points of the conjugation action are precisely commuting elements. Apply Burnside. Context clue: $1/[G : Z(G)]$ is weird, right? Use that $[G : Z(G)] = \#G/\#Z(G)$, so try to look for $\#Z(G)/\#(G)$ somewhere. Count sizes of centralizers.

Solution:

Proof (Part a).

- Define a sample space $\Omega = G \times G$, so $\#\Omega = (\#G)^2$.
- Identify the event we want to analyze:

$$A := \left\{ (g,h) \in G \times G \;\middle|\; [g,h] = 1 \right\} \subseteq \Omega.$$

- Note that the slices are centralizers:

$$A_g := \left\{ (g,h) \in \{g\} \times G \;\middle|\; [g,h] = 1 \right\} = Z(g) \implies A = \coprod_{g \in G} Z(g).$$

- Set n be the number of conjugacy classes, note we want to show $P(A) = n/|G|$.
- Let G act on itself by conjugation, which partitions G into conjugacy classes.
  - What are the orbits?

$$\mathcal{O}_g = \left\{ hgh^{-1} \;\middle|\; h \in G \right\},$$

    which is the **conjugacy class** of g. In particular, the number of orbits is the number of conjugacy classes.
  - What are the fixed points?

$$X^g = \left\{ h \in G \;\middle|\; hgh^{-1} = g \right\},$$

    which are the elements of G that commute with g, which is isomorphic to A_g.
- Identifying centralizers with fixed points,

$$\#A = \# \coprod_{g \in G} Z(g) = \sum_{g \in G} \#Z(g) = \sum_{g \in G} \#X^g.$$

- Apply Burnside

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

- Note $\#X/G = n$, i.e. the number of conjugacy classes is the number of orbits.
- Rearrange and use definition:

$$n \cdot \#G = (\#X/G) \cdot \#G = \sum_{g \in G} \#X^g$$

- Compute probability:

$$P(A) = \frac{\#A}{\#\Omega} = \sum_{g \in G} \frac{\#X^g}{(\#G)^2} = \frac{(\#X/G) \cdot \#G}{(\#G)^2} = \frac{n \cdot \#G}{(\#G)^2} = \frac{n}{\#G}.$$

■

Proof (Part b).
Statement of the class equation:

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

where $Z(x) = \left\{ g \in G \,\middle|\, [g, x] = 1 \right\}$ is the centralizer of x in G. ■

Proof (Part c).

(DZG): I couldn't convince myself that a previous proof using the class equation actually works. Instead, I'll borrow the proof from this note

- Write the event as $A = \coprod_{g \in G} \{g\} \times Z(g)$, then

$$P(A) = \frac{\#A}{(\#G)^2} = \frac{1}{(\#G)^2} \sum_{g \in G} \#Z(g).$$

- Attempt to estimate the sum: pull out central elements $g \in Z(G)$.
  - Note $Z(g) = G$ for central g, so $\#Z(g) = \#G$
  - Note

$$g \notin Z(G) \implies \#Z(g) \leq \frac{1}{2} \#G,$$

since $Z(g) \leq G$ is a subgroup, and

$$[G : Z(g)] \neq 1 \implies [G : Z(g)] \geq 2.$$

- Use these facts to calculate:

$$\begin{aligned}
P(A) &= \frac{1}{(\#G)^2} \left(\sum_{g \in Z(g)} \#Z(g) + \sum_{g \notin Z(g)} \#Z(g) \right) \\
&= \frac{1}{(\#G)^2} \left(\sum_{g \in Z(g)} \#G + \sum_{g \notin Z(g)} \#Z(g) \right) \\
&= \frac{1}{(\#G)^2} \left(\#Z(G) \cdot \#G + \sum_{g \notin Z(g)} \#Z(g) \right) \\
&\leq \frac{1}{(\#G)^2} \left(\#Z(G) \cdot \#G + \sum_{g \notin Z(g)} \frac{1}{2} \#G \right) \\
&= \frac{1}{(\#G)^2} \left(\#Z(G) \cdot \#G + \left(\sum_{g \notin Z(g)} \frac{1}{2} \right) \cdot \#G \right) \\
&= \frac{1}{(\#G)} \left(\#Z(G) + \sum_{g \notin Z(g)} \frac{1}{2} \right) \\
&= \frac{1}{(\#G)} \left(\#Z(G) + \frac{1}{2} \sum_{g \notin Z(g)} 1 \right) \\
&= \frac{1}{(\#G)} \left(\#Z(G) + \frac{1}{2} \#(G \setminus Z(G)) \right) \\
&= \frac{1}{(\#G)} \left(\#Z(G) + \frac{1}{2} \#G - \frac{1}{2} \#Z(G) \right) \\
&= \frac{1}{(\#G)} \left(\frac{1}{2} \#Z(G) + \frac{1}{2} \#G \right) \\
&= \frac{1}{2} \left(1 + \frac{\#Z(G)}{\#G} \right) \\
&= \frac{1}{2} \left(1 + \frac{1}{[G : Z(G)]} \right).
\end{aligned}$$

Redo part c

2.3 Group Actions / Representations

2.3.1 Spring 2017 #1 ✨

Let G be a finite group and $\pi : G \to \mathrm{Sym}(G)$ the Cayley representation.

(Recall that this means that for an element $x \in G$, $\pi(x)$ acts by left translation on G.)

Prove that $\pi(x)$ is an odd permutation $\iff$ the order $|\pi(x)|$ of $\pi(x)$ is even and $|G|/|\pi(x)|$ is odd.

⚠ Warning 2.3.1

(DZG): This seems like an unusually hard group theory problem. My guess is this year's qual class spent more time than usual on the proof of Cayley's theorem.

Concepts Used:

- $\mathrm{Sym}(G) \coloneqq \underset{\mathsf{Set}}{\mathrm{Aut}}(G, G)$ is the group of set morphisms from G to itself, i.e. permutations of elements of G.
- More standard terminology: this is related to the **left regular representation** where $g \mapsto \varphi_g$ where $\varphi_g(x) = gx$, regarded instead as a permutation representation.
  - This action is transitive!
- Cayley's theorem: every G is isomorphic to a subgroup of a permutation group. In particular, take $\left\{ \varphi_g \,\middle|\, G \in G \right\}$ with function composition as a subgroup of $\underset{\mathsf{Set}}{\mathrm{Aut}}(G)$.

Solution:

(DZG): Warning!! I haven't checked this solution very carefully, and this is kind of a delicate parity argument. Most of the key ideas are borrowed from here.

- Write $k \coloneqq o(\pi_g)$, then since π is injective, $k = o(g)$ in G.
- Since π_g as a cycle is obtained from the action of g, we can pick an element x_0 in G, take the orbit under the action, and obtain a cycle of length k since the order of g is k. Then continue by taking any x_1 not in the first orbit and taking *its* orbit. Continuing this way exhausts all group elements and yields a decomposition into disjoint cycles:

$$\pi_g = (x_0, gx_0, g^2x_0, \cdots, g^{k-1}x_0)(x_1, gx_1, g^2x_1, \cdots, g^{k-1}x_1) \cdots (x_m, gx_m, g^2x_m, \cdots, g^{k-1}x_m).$$

- So there are m orbits all of length exactly k. Proceed by casework.

- If k is even:
  - This yields m odd cycles, and thus π has zero (an even number) of even cycles.
  - Thus $\pi \in \ker \operatorname{sgn}$ and is an even permutation.
- If k is odd
  - This yields m even cycles, thus an even number of even cycles iff m is even
- The claim is that the number of orbit representatives m is equal to $[G : H] = \#G/H$ for $H = \langle g \rangle$.
  - Proof: define a map

$$\begin{aligned} \{\text{Orbit representatives } x_i\} &\to G/H \\ x &\mapsto xH. \end{aligned}$$

  - This is injective and surjective because

$$\begin{aligned} xH = yH &\iff xy^{-1} \in H = \langle g \rangle \\ &\iff xy^{-1} = g^{\ell} \\ &\iff x = g^{\ell} y \\ &\iff y \in \mathcal{O}_x, \end{aligned}$$

    so y and x are in the same orbit and have the same orbit representative.
- We now have

$$\pi_g \text{ is an even permutation} \iff \begin{cases} k \text{ is odd and } m \text{ is even} \\ \text{ or} \\ k \text{ is even} & . \end{cases}$$

- Everything was an iff, so flip the evens to odds:

$$\pi_g \text{ is an odd permutation} \iff \begin{cases} k \text{ is even and } m \text{ is odd} \\ \text{ or} & . \\ k \text{ is odd} & . \end{cases}$$

- Then just recall that $k := o(\pi_g)$ and

$$m = [G : \langle g \rangle] = \#G/\# \langle g \rangle = \#G/o(g) = \#G/o(\pi_g).$$

2.3.2 Fall 2015 #1 ✨

Let G be a group containing a subgroup H not equal to G of finite index. Prove that G has a normal subgroup which is contained in every conjugate of H which is of finite index.

(DZG) A remark: it's not the conjugates that should be finite index here, but rather the normal subgroup.

Solution:

- Let $H \leq G$ and define $n := [G : H]$.
- Write $G/H = \{x_1 H, \cdots, x_n H\}$ for the finitely many cosets.
- Let G act on G/H by left translation, so $g \cdot xH := gxH.$. Call the action $\psi : G \to \operatorname{Sym}(G/H)$.
- Then $\operatorname{Stab}(xH) = xHx^{-1}$ is a subgroup conjugate to H, and $K := \ker \psi = \bigcap_{i=1}^{n} xHx^{-1}$ is the intersection of all conjugates of H.
- Kernels are normal, so $K \trianglelefteq G$, and $K \subseteq xHx^{-1}$ for all x, meaning K is contained in every conjugate of H.
- The index $[G : K]$ is finite since $G/K \cong \operatorname{im} \psi$ by the first isomorphism theorem, and $\# \operatorname{im} \psi \leq \# \operatorname{Sym}(G/H) = \# S_n = n! < \infty$.

2.4 Conjugacy Classes

2.4.1 Spring 2021 #2 ✨

Let $H \trianglelefteq G$ be a normal subgroup of a finite group G, where the order of H is the smallest prime p dividing $|G|$. Prove that H is contained in the center of G.

Solution due to Swaroop Hegde, typed up + modifications added by DZG.

Concepts Used:

- $x \in Z(G)$ iff $\# C_x = 1$, i.e. the size of its conjugacy class is one.
- Normal subgroups are disjoint unions of (some) conjugacy classes in G.
  - In fact, this is a characterization of normal subgroups (i.e. H is normal iff H is a union of conjugacy classes in G).
  - Why: if $H \trianglelefteq G$ then $ghg^{-1} \in H$ for all g, so $C_h \subseteq H$ and $\bigcup_h C_h = H$. Conversely, if $H = \bigcup_{h \in H} C_h$, then $ghg^{-1} \in C_h \subseteq H$ and thus $gHg^{-1} = H$.
- Orbit stabilizer theorem: $\# C_g = \# G / \# K_g$ where C_g is the centralizer and K_g is the conjugacy class of g.
  - In particular, $\# C_g$ divides $\# G$.

Strategy:
Show an element x is central by showing $\# C_x = 1$.

Proof (?).

- Let $p := \#H$.
- Let $\{C_i\}_{i\leq n}$ be the conjugacy classes in G, then $G = \coprod_{i\leq n} C_i$
- By the first fact, there is a sub-collection $\left\{C_{i_j}\right\}_{j\leq k}$ such that

$$H = \textstyle\coprod_{j\leq k} C_{i_j}.$$

- The identity is always in a single conjugacy class, so $C_e = \{e\}$.
- Since $e \in H$, without loss of generality, label $C_{i_1} = \{e\}$.
- So

$$H = \coprod_{j\leq k} C_{i_j} = C_{i_1} \coprod \coprod_{\substack{j\leq k \\ j\neq 1}} C_{i_j}.$$

- Take cardinality in the above equation

$$p = 1 + \sum_{\substack{j\leq k \\ j\neq 1}} \#C_{i_j}.$$

- So $\#C_{i_j} \leq p-1$ for all $j \neq 1$.
- Every $\#C_{i_j}$ divides $\#G$, but p was the *minimal* prime dividing $\#G$, forcing $\#C_{i_j} = 1$ for all $j \neq 1$.
  - This rules out $\#C_{i_j}$ being a prime less than p, but also rules out composites: if a prime $q \mid \#C_{i_j}$, then $q < p$ and $q \mid \#G$, a contradiction.
- By fact 3, each $x \in C_{i_j}$ satisfies $x \in Z(G)$.
- $\cup C_{i_j} = H$, so $H \subseteq Z(G)$.

■

2.4.2 Spring 2015 #1 ✨

For a prime p, let G be a finite p-group and let N be a normal subgroup of G of order p. Prove that N is contained in the center of G.

Concepts Used:

- Definition of conjugacy class: $[x] = \left\{gxg^{-1} \;\middle|\; g \in G\right\}$.
- A conjugacy class $[x]$ is trivial iff $[x] = \{x\}$ iff $x \in Z(G)$.

- Sizes of conjugacy classes divide the order of the group they live in.
    - This is orbit-stabilizer: $G \curvearrowright G$ by $g \cdot x := gxg^{-1}$, so $\mathcal{O}(x) = [x]$. Then $\#\mathcal{O}(x) = \#G/\#\mathrm{Stab}(x)$, so $\#\mathcal{O}(x)$ divides $\#G$.

Solution:

- Use that $N \trianglelefteq G \iff N = \coprod'[n_i]$ is a *disjoint* union of (full) conjugacy classes.
- Take cardinalities:

$$p = \#N = \sum_{i=1}^{m} \#[n_i] = 1 + \sum_{i=2}^{m} [n_i].$$

- The size of each conjugacy class divides the size of H by orbit-stabilizer, so $\#[n_i] \mid p$ for each i.
- But the entire second term must sum to $p-1$ for this equality to hold, which forces $\#[n_i] = 1$ (and incidentally $m = p-1$)
- Then $[n_i] = \{n_i\} \iff n_i \in Z(G)$, and this holds for all i, so $N \subseteq Z(G)$.

2.5 Unsorted / Counting Arguments

2.5.1 Fall 2019 Midterm #5 ✨

Let G be a nonabelian group of order p^3 for p prime. Show that $Z(G) = [G, G]$.

Note: this is a good problem, it tests several common theorems at once. Proof due to Paco Adajar.

Concepts Used:
Important notations and definitions:

- The **center** of G, denoted by $Z(G)$, is the subset of elements of G which commute with all elements of G. That is, if $x \in Z(G)$, then for all $g \in G$, $gx = xg$:

  $$Z(G) = \{x \in G : gx = xg \text{ for all } g \in G\}.$$

  In fact, $Z(G)$ is not just a subset of G, but a normal subgroup of G.

- The **commutator subgroup** of G, denoted by $[G, G]$, is the subgroup of G generated by the commutators of G, i.e., the elements of the form $ghg^{-1}h^{-1}$:

  $$[G, G] = \langle ghg^{-1}h^{-1} : g, h \in G \rangle.$$

  The commutator subgroup $[G, G]$ is the smallest normal subgroup of G whose quotient is abelian. That is, if H is a normal subgroup of G for which G/H is abelian, then $[G, G] \leq H$.

Moreover, G is abelian if and only if $[G, G]$ is trivial.

Theorems to remember and know how to prove:

- $G/Z(G)$ **Theorem**: If $G/Z(G)$ is cyclic, then G is abelian, i.e., $G/Z(G)$ is in fact trivial.
- **Lagrange's Theorem**: If G is a group of finite order and H is a subgroup of G, then the order of H divides that of G.
  - One consequence of this is that every group of prime order is cyclic.
- A p-group (a group of order p^n for some prime p and some positive integer n) has nontrivial center.
- A consequence of the theorems above: every group of order p^2 (where p is prime) is abelian.

Solution:
Since $Z(G)$ is a subgroup of G and $|G| = p^3$, by Lagrange's theorem, $|Z(G)| \in \{1, p, p^2, p^3\}$. Since we stipulated that G is nonabelian, $|Z(G)| \neq p^3$. Also, since G is a p-group, it has nontrivial center, so $|Z(G)| \neq 1$. Finally, by the $G/Z(G)$ theorem, $|Z(G)| \neq p^2$: if $|Z(G)| = p^2$, then $|G/Z(G)| = p$ and so $G/Z(G)$ would be cyclic, meaning that G is abelian. Hence, $|Z(G)| = p$.
Then, since $|Z(G)| = p$, we have that $|G/Z(G)| = p^2$, and so $G/Z(G)$ is abelian. Thus, $[G, G] \in Z(G)$. Since $|Z(G)| = p$, then $|[G, G]| \in \{1, p\}$ again by Lagrange's theorem. If $|[G, G]| = p$ then $[G, G] = Z(G)$ and we are done. And, indeed, we must have $|[G, G]| = p$, because G is nonabelian and so $|[G, G]| \neq 1$.

2.5.2 Spring 2012 #2 ✨

Let G be a finite group and p a prime number such that there is a normal subgroup $H \trianglelefteq G$ with $|H| = p^i > 1$.

a. Show that H is a subgroup of any Sylow p-subgroup of G.

b. Show that G contains a nonzero abelian normal subgroup of order divisible by p.

Concepts Used:

- p groups have nontrivial centers.
- Definition of maximality and p-groups
- Sylows are conjugate
- $Z(G) \operatorname{ch} G$ always.
- Transitivity of characteristic: $A \operatorname{ch} B$ and $B \trianglelefteq C$ implies $A \trianglelefteq C$.

Strategy:

Just use maximality for (a). For (b), centers are always abelian, so $Z(H)$ is good to consider, just need to ensure it's normal in G. Use transitivity of characteristic.

Solution:

Proof (of a).

- By definition, $S \in \operatorname{Syl}_p(G) \iff S$ is a *maximal* p-subgroup: $S < G$ is a p-group, so $\#S = p^k$ for some k, S is a proper subgroup, and S is maximal in the sense that there are no proper p-subgroups S' with $S \subsetneq S' \subsetneq G$.
- Since $\#H = p^i$, H is a p-subgroup of G.
- If H is maximal, then by definition $H \in \operatorname{Syl}_p(G)$
- Otherwise, if H is not maximal, there exists an $H' \supsetneq H$ with $H' \leq G$ a p-subgroup properly containing H.
    - In this apply the same argument to H': this yields a proper superset containment at every stage, and since G is finite, there is no infinite ascending chain of proper supersets.
    - So this terminates in some maximal p-subgroup S, i.e. a Sylow p-subgroup.
- So $H \subseteq S$ for some $S \in \operatorname{Syl}_p(G)$.
- All Sylows are conjugate, so for any $S' \in \operatorname{Syl}_p(G)$ we can write $S' = gSg^{-1}$ for some g.
- Then using that H is normal, $H \subseteq S \implies H = gHg^{-1} \subseteq gSg^{-1} \coloneqq S'$. So H is contained in every Sylow p-subgroup.

■

Proof (of b).

- Claim: $Z(H) \leq H$ works.
  - It is nontrivial since H is a p-group and p-groups have nontrivial centers
  - It is abelian since $Z(Z(H)) = Z(H)$.
  - $\# Z(H) = p^\ell$ for some $\ell \leq i$ by Lagrange
- It thus remains to show that $Z(H) \trianglelefteq G$.
- Use that $Z(H) \operatorname{ch} H$ and use transitivity of characteristic to conclude $Z(H) \trianglelefteq H$.
- That $Z(H) \operatorname{ch} H$: let $\psi \in \operatorname{Aut}(H)$ and $x = \psi(y) \in \psi(Z(H))$ so $y \in Z(H)$, then for arbitrary $h \in H$,

$$\begin{aligned}
\psi(y)h &= \psi(y)(\psi \circ \psi^{-1})(h) \\
&= \psi(y \cdot \psi^{-1}(h)) \\
&= \psi(\psi^{-1}(h) \cdot y) && \text{since } \psi^{-1}(h) \in H,\ y \in Z(H) \\
&= h\psi(y).
\end{aligned}$$

- That $A \operatorname{ch} B \trianglelefteq C \implies A \trianglelefteq C$:
  - $A \operatorname{ch} B$ 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 $\psi(-) := c(-)c^{-1}$ descends to an element of $\operatorname{Aut}(B)$.
  - Then $\psi(A) = A$ since $A \operatorname{ch} B$, so $cAc^{-1} = A$ and $A \trianglelefteq C$.

■

2.5.3 Fall 2016 #1 ✨

Let G be a finite group and $s, t \in G$ be two distinct elements of order 2. Show that subgroup of G generated by s and t is a dihedral group.

Recall that the dihedral groups of order $2m$ for $m \geq 2$ are of the form

$$D_{2m} = \left\langle \sigma, \tau \;\middle|\; \sigma^m = 1 = \tau^2, \tau\sigma = \sigma^{-1}\tau \right\rangle.$$

Solution:

- Suppose $G = \langle a, b \rangle$ with $a^2 = b^2 = e$, satisfying some unknown relations.
- Consider ab. Since G is finite, this has finite order, so $(ab)^n = e$ for some $n \geq 2$.
- Note $\langle ab, b \rangle \subseteq \langle a, b \rangle$, since any finite word in ab, b is also a finite word in a, b.
- Since $(ab)b = ab^2 = a$, we have $\langle ab, b \rangle \subseteq \langle a, b \rangle$, so $\langle ab, b \rangle = \langle a, b \rangle$.

- Write $D_{2n} = F(r, s)/ \ker \pi$ for $\pi : F(r, s) \to D_{2n}$ the canonical presentation map.
- Define

$$\begin{aligned} \psi : F(r,s) &\to G \\ r &\mapsto ab \\ t &\mapsto b. \end{aligned}$$

- This is clearly surjective since it hits all generators.
- We'll show that ab, a satisfy all of the relations defining D_{2n}, which factors ψ through $\ker \pi$, yielding a surjection $\tilde{\psi} : D_{2n} \twoheadrightarrow G$.
  - $(ab)^n = e$ by construction, $b^2 = e$ by assumption, and

$$b(ab)b^{-1} = babb^{-1} = ba = b^{-1}a^{-1} = (ab)^{-1},$$

    corresponding to the relation $srs^{-1} = r^{-1}$. Here we've used that $o(a) = o(b) = 2$ implies $a = a^{-1}, b = b^{-1}$.
- Surjectivity of $\tilde{\psi}$ yields $2n = \#D_{2n} \geq \#G$.
- The claim is that $\#G \geq 2n$, which forces $\#G = 2n$. Then $\tilde{\psi}$ will be a surjective group morphism between groups of the same order, and thus an isomorphism.
  - We have $\langle ab \rangle \leq G$, so $n \mid \#G$.
  - Since $b \notin \langle ab \rangle$, this forces $\#G > n$, so $\#G \geq 2n$.

Remark: see a more direct proof in Theorem 2.1 and Theorem 1.1 here

2.5.4 Fall 2019 Midterm #1 ✨

Let G be a group of order $p^2 q$ for p, q prime. Show that G has a nontrivial normal subgroup. :::

Solution:

- Write $\#G = p^2 q$
- Cases: first assume $p > q$, then do $q < p$.
- In any case, we have

$$n_p \mid q \implies n_p \in \{1, q\}$$

$$n_q \mid p^2 \implies n_q \in \left\{1, p, p^2\right\}.$$

- If $n_p = 1$ or $n_q = 1$, we're done, so suppose otherwise.

- **Case 1:** : $p > q$.
  - Using that $[n_p]_p \equiv 1$, consider reducing elements in $\{1, q\} \bmod p$.
  - Since $q < p$, we just have $q \bmod p = q$, and as long as $q \neq 1$ we have $q \not\equiv 1 \bmod p$. But since $n_p \neq 1$ and $n_p \neq q$, this is a contradiction. ↯

- **Case 2:** $p < q$:
  - Using that $[n_q]_q \equiv 1$, consider reducing $\left\{1, p, p^2\right\} \bmod q$.
  - Since now $p < q$, we have $p \bmod q = p$ itself, so $p \bmod q \neq 1$ and we can rule it out.
  - The remaining possibility is $n_q = p^2$.
  - Supposing that $n_p \neq 1$, we have $n_p = q$, so we can count

    $$\text{Elements from Sylow } q : n_q(\#S_q - 1) = p^2(q-1) + 1,$$

    where we've used that distinct Sylow qs can only intersect at the identity, and although Sylow ps *can* intersect trivially, they can also intersect in a subgroup of size p.
  - Suppose all Sylow ps intersect trivially, we get at least

    $$\text{Elements from Sylow } p : n_p(\#S_p - 1) = q(p^2 - 1).$$

    Then we get a count of how many elements the Sylow ps and qs contribute:

    $$q(p^2-1) + p^2(q-1) + 1 = p^2 q - q + p^2 q - p^2 + 1 = p^2 q + (p^2-1)(q-1) > p^2 q = \#G,$$

    provided $(p^2-1)(q-1) \neq 0$, which is fine for $p \geq 2$ since this is at least $(2^2-1)(3-2) = 3$ (since $p < q$ and $q = 3$ is the next smallest prime). ↯
  - Otherwise, we get two Sylow ps intersecting nontrivially, which must be in a subgroup of order at least p since the intersection is a subgroup of both. In this case, just considering these two subgroups, we get

    $$\text{Elements from Sylow } p : n_p(\#S_p - 1) > p^2 + p^2 - p = 2p^2 - p - 1.$$

    Then a count:

    $$\begin{aligned} p^2(q-1) + (2p^2 - p - 1) + 1 &= p^2 q - p^2 + 2p^2 - p \\ &= p^2 q + p^2 - p \\ &= p^2 q + p(p-1) \\ &> p^2 q = \#G, \end{aligned}$$

    a contradiction since this inequality is strict provided $p \geq 2$. ↯

2.5.5 Fall 2019 Midterm #4

Let p be a prime. Show that $S_p = \langle \tau, \sigma \rangle$ where τ is a transposition and σ is a p-cycle.

3 | Groups: Group Actions

3.1 Fall 2012 #1

Let G be a finite group and X a set on which G acts.

a. Let $x \in X$ and $G_x \coloneqq \left\{ g \in G \;\middle|\; g \cdot x = x \right\}$. Show that G_x is a subgroup of G.

b. Let $x \in X$ and $G \cdot x \coloneqq \left\{ g \cdot x \;\middle|\; g \in G \right\}$. Prove that there is a bijection between elements in $G \cdot x$ and the left cosets of G_x in G.

3.2 Fall 2015 #2

Let G be a finite group, H a p-subgroup, and P a sylow p-subgroup for p a prime. Let H act on the left cosets of P in G by left translation.

Prove that this is an orbit under this action of length 1.

Prove that xP is an orbit of length 1 $\iff$ H is contained in xPx^{-1}.

3.3 Spring 2016 #5

Let G be a finite group acting on a set X. For $x \in X$, let G_x be the stabilizer of x and $G \cdot x$ be the orbit of x.

a. Prove that there is a bijection between the left cosets G/G_x and $G \cdot x$.

b. Prove that the center of every finite p-group G is nontrivial by considering that action of G on $X = G$ by conjugation.

3.4 Fall 2017 #1 🚩

Suppose the group G acts on the set A. Assume this action is faithful (recall that this means that the kernel of the homomorphism from G to $\mathrm{Sym}(A)$ which gives the action is trivial) and transitive (for all a, b in A, there exists g in G such that $g \cdot a = b$.)

a. For $a \in A$, let G_a denote the stabilizer of a in G. Prove that for any $a \in A$,

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = \{1\} .$$

b. Suppose that G is abelian. Prove that $|G| = |A|$. Deduce that every abelian transitive subgroup of S_n has order n.

3.5 Fall 2018 #2 ✨

a. Suppose the group G acts on the set X . Show that the stabilizers of elements in the same orbit are conjugate.

b. Let G be a finite group and let H be a proper subgroup. Show that the union of the conjugates of H is strictly smaller than G, i.e.

$$\bigcup_{g \in G} gHg^{-1} \subsetneq G$$

c. Suppose G is a finite group acting transitively on a set S with at least 2 elements. Show that there is an element of G with no fixed points in S.

Concepts Used:

- Orbit: $G \cdot x \coloneqq \left\{ g \cdot x \;\middle|\; g \in G \right\} \subseteq X$
- Stabilizer: $G_x \coloneqq \left\{ g \in G \;\middle|\; g \cdot x = x \right\} \leq G$
- Orbit-Stabilizer: $G \cdot x \simeq G/G_x$.
- $abc \in H \iff b \in a^{-1}Hc^{-1}$
- Set of orbits for $G \curvearrowright X$, notated X/G.
- Set of fixed points for $G \curvearrowright X$, notated X^g.
- Burnside's Lemma: $|X/G| \cdot |G| = \sum_{g \in G} |X^g|$
    - Number of orbits equals average number of fixed points.

Solution:

Proof (of a).

- Fix x, then $y \in \mathrm{Orb}(x) \implies g \cdot x = y$ for some g, and $x = g^{-1} \cdot y$.
- Then

$$\begin{aligned} h \in \mathrm{Stab}(x) &\iff h \cdot x = x && \text{by being in the stabilizer} \\ &\iff h \cdot (g^{-1} \cdot y) = g^{-1} \cdot y \\ &\iff (ghg^{-1}) \cdot y = y \\ &\iff ghg^{-1} \in G_y && \text{by definition} \\ &\iff h \in g^{-1}\mathrm{Stab}(y)g, \end{aligned}$$

so $\mathrm{Stab}(x) = g^{-1}\mathrm{Stab}(y)g$.

■

Proof (of b).
Let G act on its subgroups by conjugation,

- The orbit $G \cdot H$ is the set of all subgroups conjugate to H, and
- The stabilizer of H is $G_H = N_G(H)$.
- By orbit-stabilizer,

$$G \cdot H = [G : G_H] = [G : N_G(H)].$$

- Since $|H| = n$, and all of its conjugate also have order n.
- Note that

$$H \leq N_G(H) \implies |H| \leq |N_G(H)| \implies \frac{1}{|N_G(H)|} \leq \frac{1}{|H|},$$

- Now *strictly* bound the size of the union by overcounting their intersections at the identity:

$$\begin{aligned}\left| \bigcup_{g \in G} gHg^{-1} \right| &< (\text{Number of Conjugates of } H) \cdot (\text{Size of each conjugate}) \\ &\text{strictly overcounts since they intersect in at least the identity} \\ &= [G : N_G(H)]|H| \\ &= \frac{|G|}{|N_G(H)|}|H| \\ &\text{since } G \text{ is finite} \\ &\leq \frac{|G|}{|H|}|H| \\ &= |G|.\end{aligned}$$

■

Proof (of c).

- Let $G \curvearrowright X$ transitively where $|X| \geq 2$.
- An action is transitive iff there is only one orbit, so $|X/G| = 1$.
- Apply Burnside's Lemma

$$1 = |X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| \implies |G| = \sum_{g \in G} |\mathrm{Fix}(g)| = \mathrm{Fix}(e) + \sum_{\substack{g \in G \\ g \neq e}} |\mathrm{Fix}(g)|$$

- Note that $\mathrm{Fix}(e) = X$, since the identity must fix every element, so $|\mathrm{Fix}(e)| \geq 2$.
- If $|\mathrm{Fix}(g)| > 0$ for all $g \neq e$, the remaining term is at least $|G| - 1$. But then the right-hand side yields is at least $2 + (|G| - 1) = |G| + 1$, contradicting the equality.
- So not every $|\mathrm{Fix}(g)| > 0$, and $|\mathrm{Fix}(g)| = 0$ for some g, which says g has no fixed points in X.

■

4 Groups: Sylow Theory

4.1 Fall 2019 #1 ✨

Let G be a finite group with n distinct conjugacy classes. Let $g_1 \cdots g_n$ be representatives of the conjugacy classes of G. Prove that if $g_i g_j = g_j g_i$ for all i, j then G is abelian.

Concepts Used:

- $Z(g) = G \iff g \in Z(G)$, i.e. if the centralizer of g is the whole group, g is central.
- If $H \leq G$ is a *proper* subgroup, then $\bigcup_{g \in G} hGh^{-1}$ is again a proper subgroup (subset?) I.e. G is not a union of conjugates of any proper subgroup.
- So if G *is* a union of conjugates of H, then H must not be proper, i.e. $H = G$.

Solution:

- We have $g_j \subseteq Z(g_k)$ for all k by assumption.
- If we can show $Z(g_k) = G$ for all k, then $g_k \in Z(G)$ for all k.
  - Then each conjugacy class is size 1, and since $G = \coprod_{i=1}^{n} [g_i] = \coprod_{i=1}^{n} \{g_i\}$, every $g \in G$ is some g_i. So $G \subseteq Z(G)$, forcing G to be abelian.

- If we can show $G \subseteq \bigcup_{h\in H} hZ(g_k)h^{-1}$ for some k, this forces $Z(g_k) = G$ and $g_k \in Z(G)$.
  - If we can do this for all k, we're done!
- Since $g \in G$ is in some conjugacy class, write $g = hg_jh^{-1}$ for some $h \in G$ and some $1 \leq j \leq n$.
- Now use $g_j \in Z(g_k)$ for all k:

$$\begin{aligned} g \in G &\implies g = hg_jh^{-1} && \text{for some } h \in H \\ g_j \in Z(g_k) \forall k &\implies g \in hZ(g_k)h^{-1} && \text{for some } h, \forall 1 \leq k \leq n \\ &\implies g \in \bigcup_{h\in G} hZ(g_k)h^{-1} && \forall 1 \leq k \leq n \end{aligned}$$

.

  - Note that it's necessary to get rid of the h dependence, since now now every $g \in G$ is in $\bigcup_{h\in G} hZ(g_k)h^{-1}$.
- Now

$$G \subseteq \bigcup_{h\in G} hZ(g_k) \subseteq G \ \forall k \implies Z(g_k) = G \ \forall k,$$

and we're done.

4.2 Fall 2019 Midterm #2

Let G be a finite group and let P be a sylow p-subgroup for p prime. Show that $N(N(P)) = N(P)$ where N is the normalizer in G.

4.3 Fall 2013 #2

Let G be a group of order 30.

a. Show that G has a subgroup of order 15.

b. Show that every group of order 15 is cyclic.

c. Show that G is isomorphic to some semidirect product $\mathbb{Z}_{15} \rtimes \mathbb{Z}_2$.

d. Exhibit three nonisomorphic groups of order 30 and prove that they are not isomorphic. You are not required to use your answer to (c).

4.4 Spring 2014 #2

Let $G \subset S_9$ be a Sylow-3 subgroup of the symmetric group on 9 letters.

a. Show that G contains a subgroup H isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ by exhibiting an appropriate set of cycles.

b. Show that H is normal in G.

c. Give generators and relations for G as an abstract group, such that all generators have order 3. Also exhibit elements of S_9 in cycle notation corresponding to these generators.

d. Without appealing to the previous parts of the problem, show that G contains an element of order 9.

4.5 Fall 2014 #2

Let G be a group of order 96.

a. Show that G has either one or three 2-Sylow subgroups.

b. Show that either G has a normal subgroup of order 32, or a normal subgroup of order 16.

4.6 Spring 2016 #3

a. State the three Sylow theorems.

b. Prove that any group of order 1225 is abelian.

c. Write down exactly one representative in each isomorphism class of abelian groups of order 1225.

4.7 Spring 2017 #2

a. How many isomorphism classes of abelian groups of order 56 are there? Give a representative for one of each class.

b. Prove that if G is a group of order 56, then either the Sylow-2 subgroup or the Sylow-7 subgroup is normal.

c. Give two non-isomorphic groups of order 56 where the Sylow-7 subgroup is normal and the Sylow-2 subgroup is *not* normal. Justify that these two groups are not isomorphic.

4.8 Fall 2017 #2 🚩

a. Classify the abelian groups of order 36.

For the rest of the problem, assume that G is a non-abelian group of order 36. You may assume that the only subgroup of order 12 in S_4 *is* A_4 *and that* A_4 *has no subgroup of order 6.*

b. Prove that if the 2-Sylow subgroup of G is normal, G has a normal subgroup N such that G/N is isomorphic to A_4.

c. Show that if G has a normal subgroup N such that G/N is isomorphic to A_4 and a subgroup H isomorphic to A_4 it must be the direct product of N and H.

d. Show that the dihedral group of order 36 is a non-abelian group of order 36 whose Sylow-2 subgroup is not normal.

4.9 Fall 2012 #2 🚩

Let G be a group of order 30.

a. Show that G contains normal subgroups of orders 3, 5, and 15.

b. Give all possible presentations and relations for G.

c. Determine how many groups of order 30 there are up to isomorphism.

4.10 Fall 2018 #1 ✨

Let G be a finite group whose order is divisible by a prime number p. Let P be a normal p-subgroup of G (so $|P| = p^c$ for some c).

a. Show that P is contained in every Sylow p-subgroup of G.

b. Let M be a maximal proper subgroup of G. Show that either $P \subseteq M$ or $|G/M| = p^b$ for some $b \leq c$.

Concepts Used:

- Sylow 2: All Sylow p-subgroups are conjugate.
- $|HK| = |H||K|/|H \cap K|$.
- Lagrange's Theorem: $H \leq G \implies |H| \mid |G|$

Solution:

Proof (of a).

- Every p-subgroup is contained in some Sylow p-subgroup, so $P \subseteq S_p^i$ for some $S_p^i \in \text{Syl}_p(G)$.
- $P \trianglelefteq G \iff gPg^{-1} = P$ for all $g \in G$.
- Let S_p^j be any other Sylow p-subgroup,
- Since Sylow p-subgroups are all conjugate $gS_p^i g^{-1} = S_p^j$ for *some* $g \in G$.
- Then

$$P = gPg^{-1} \subseteq gS_p^i g^{-1} = S_p^j.$$

■

Proof (of b).

- If P is not contained in M, then $M < MP$ is a proper subgroup
- By maximality of M, $MP = G$
- Note that $M \cap P \leq P$ and $|P| = p^c$ implies $|M \cap P| = p^a$ for some $a \leq c$ by Lagrange
- Then write

$$G = MP \iff |G| = \frac{|M||P|}{|M \cap P|}$$

$$\iff \frac{|G|}{|M|} = \frac{|P|}{|M \cap P|} = \frac{p^c}{p^a} = p^{c-a} := p^b$$

where $a \leq c \implies 0 \leq c - b \leq c$ so $0 \leq b \leq c$.

■

4.11 Fall 2019 #2 ✨

Let G be a group of order 105 and let P, Q, R be Sylow 3, 5, 7 subgroups respectively.

a. Prove that at least one of Q and R is normal in G.

b. Prove that G has a cyclic subgroup of order 35.

c. Prove that both Q and R are normal in G.

d. Prove that if P is normal in G then G is cyclic.

Concepts Used:

- The pqr theorem.
- Sylow 3: $|G| = p^n m$ implies $n_p \mid m$ and $n_p \cong 1 \mod p$.
- **Theorem**: If $H, K \leq G$ and any of the following conditions hold, HK is a subgroup:
  - $H \trianglelefteq G$ (wlog)
  - $[H, K] = 1$
  - $H \leq N_G(K)$

- **Theorem**: For a positive integer n, all groups of order n are cyclic $\iff$ n is squarefree and, for each pair of distinct primes p and q dividing n, $q-1 \neq 0 \bmod p$.
- **Theorem:**

$$A_i \trianglelefteq G, \quad G = A_1 \cdots A_k, \quad A_k \cap \prod_{i \neq k} A_i = \emptyset \implies G = \prod A_i.$$

- The intersection of subgroups is a again a subgroup.
- Any subgroups of coprime order intersect trivially?

Solution:

Proof (of 1).

- We have
- $n_3 \mid 5 \cdot 7, \quad n_3 \cong 1 \bmod 3 \implies n_3 \in \{1, 5, 7, 35\} \setminus \{5, 35\}$
- $n_5 \mid 3 \cdot 7, \quad n_5 \cong 1 \bmod 5 \implies n_5 \in \{1, 3, 7, 21\} \setminus \{3, 7\}$
- $n_7 \mid 3 \cdot 5, \quad n_7 \cong 1 \bmod 7 \implies n_7 \in \{1, 3, 5, 15\} \setminus \{3, 5\}$
- Thus

$$n_3 \in \{1, 7\} \quad n_5 \in \{1, 21\} \quad n_7 \in \{1, 15\}.$$

- Toward a contradiction, if $n_5 \neq 1$ and $n_7 \neq 1$, then

  $$|\mathrm{Syl}(5) \cup \mathrm{Syl}(7)| = (5-1)n_5 + (7-1)n_7 + 1 = 4(21) + 6(15) = 174 > 105 \text{ elements}$$

  using the fact that Sylow p-subgroups for distinct primes p intersect trivially (?).

■

Proof (of 2).

- By (a), either Q or R is normal.
- Thus $QR \leq G$ is a subgroup, and it has order $|Q| \cdot |R| = 5 \cdot 7 = 35$.
- By the pqr theorem, since 5 does not divide $7 - 1 = 6$, QR is cyclic.

■

Part (b) not finished!

Proof (of 3).

- We want to show $Q, R \trianglelefteq G$, so we proceed by showing **not** $(n_5 = 21 \text{ or } n_7 = 15)$, which is equivalent to $(n_5 = 1 \text{ and } n_7 = 1)$ by the previous restrictions.
- Note that we can write

$$G = \{\text{elements of order } n\} \coprod \{\text{elements of order not } n\}.$$

for any n, so we count for $n = 5, 7$:

  - Elements in QR of order **not** equal to 5: $|QR - Q\{\text{id}\} + \{\text{id}\}| = 35 - 5 + 1 = 31$
  - Elements in QR of order **not** equal to 7: $|QR - \{\text{id}\} R + \{\text{id}\}| = 35 - 7 + 1 = 29$

- Since $QR \leq G$, we have
  - Elements in G of order **not** equal to $5 \geq 31$.
  - Elements in G of order **not** equal to $7 \geq 29$.
- Now both cases lead to contradictions:
  - $n_5 = 21$:

$$\begin{aligned} |G| &= |\{\text{elements of order } 5\} \coprod \{\text{elements of order not } 5\}| \\ &\geq n_5(5-1) + 31 = 21(4) + 31 = 115 > 105 = |G|. \end{aligned}$$

  - $n_7 = 15$:

$$\begin{aligned} |G| &= |\{\text{elements of order } 7\} \coprod \{\text{elements of order not } 7\}| \\ &\geq n_7(7-1) + 29 = 15(6) + 29 = 119 > 105 = |G|. \end{aligned}$$

■

Proof (of 4).
Suppose P is normal and recall $|P| = 3, |Q| = 5, |R| = 7$.

- $P \cap QR = \{e\}$ since $(3, 35) = 1$
- $R \cap PQ = \{e\}$ since $(5, 21) = 1$
- $Q \cap RP = \{e\}$ since $(7, 15) = 1$

We also have $PQR = G$ since $|PQR| = |G|$ (???).
We thus have an internal direct product

$$G \cong P \times Q \times R \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{105}.$$

by the Chinese Remainder Theorem, which is cyclic.

■

4.12 Spring 2021 #3

a. Show that every group of order p^2 with p prime is abelian.

b. State the 3 Sylow theorems.

c. Show that any group of order $4225 = 5^2 13^2$ is abelian.

d. Write down one representative from each isomorphism class of abelian groups of order 4225.

4.13 Fall 2020 #1

a. Using Sylow theory, show that every group of order $2p$ where p is prime is not simple.

b. Classify all groups of order $2p$ and justify your answer. For the nonabelian group(s), give a presentation by generators and relations.

4.14 Fall 2020 #2

Let G be a group of order 60 whose Sylow 3-subgroup is normal.

a. Prove that G is solvable.

b. Prove that the Sylow 5-subgroup is also normal.

5 | Groups: Classification

5.1 Spring 2020 #1

a. Show that any group of order 2020 is solvable.

b. Give (without proof) a classification of all abelian groups of order 2020.

c. Describe one nonabelian group of order 2020.

Work this problem.

5.2 Spring 2019 #3 ✨

How many isomorphism classes are there of groups of order 45?

Describe a representative from each class.

Concepts Used:

- Sylow theorems:
- $n_p \cong 1 \mod p$
- $n_p \mid m$.

Solution:

- It turns out that $n_3 = 1$ and $n_5 = 1$, so $G \cong S_3 \times S_5$ since both subgroups are normal.
- There is only one possibility for S_5, namely $S_5 \cong \mathbb{Z}/(5)$.
- There are two possibilities for S_3, namely $S_3 \cong \mathbb{Z}/(3^2)$ and $\mathbb{Z}/(3)^2$.
- Thus
- $G \cong \mathbb{Z}/(9) \times \mathbb{Z}/(5)$, or
- $G \cong \mathbb{Z}/(3)^2 \times \mathbb{Z}/(5)$.

Revisit, seems short.

5.3 Spring 2012 #3 🚩

Let G be a group of order 70.

a. Show that G is not simple.

b. Exhibit 3 nonisomorphic groups of order 70 and prove that they are not isomorphic.

5.4 Fall 2016 #3 🚩

How many groups are there up to isomorphism of order pq where $p < q$ are prime integers?

5.5 Spring 2018 #1 ✨

a. Use the Class Equation (equivalently, the conjugation action of a group on itself) to prove that any p-group (a group whose order is a positive power of a prime integer p) has a nontrivial center.

b. Prove that any group of order p^2 (where p is prime) is abelian.

c. Prove that any group of order $5^2 \cdot 7^2$ is abelian.

d. Write down exactly one representative in each isomorphism class of groups of order $5^2 \cdot 7^2$.

Concepts Used:

- Centralizer: $C_G(x) = \left\{ g \in G \;\middle|\; [gx] = 1 \right\}$.
- Class Equation: $|G| = |Z(G)| + \sum [G : C_G(x_i)]$
- $G/Z(G)$ cyclic $\iff$ G is abelian.

$$\begin{aligned} G/Z(G) = \langle xZ \rangle &\iff g \in G \implies gZ = x^m Z \\ &\iff g(x^m)^{-1} \in Z \\ &\iff g = x^m z \quad \text{forsome} \quad z \in Z \\ &\implies gh = x^m z_1 x^n z_2 = x^n z_2 x^m z_1 = hg. \end{aligned}$$

- Every group of order p^2 is abelian.
- Classification of finite abelian groups.

Solution:

Proof (of a).
Strategy: get p to divide $|Z(G)|$.

- Apply the class equation:

$$|G| = |Z(G)| + \sum [G : C_G(x_i)].$$

- Since $C_G(x_i) \leq G$ and $|G| = p^k$, by Lagrange $|C_G(x_i)| = p^\ell$ for some $0 \leq \ell \leq k$.
- Since $|G| = p^k$ for some k and $Z(G), C_G(x_i) \leq G$ are subgroups, their orders are powers of p.
- Use

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

  - Thus every index appearing in the sum is greater than 1, and thus equal to p^{ℓ_i} for some $1 \leq \ell_i \leq k$
  - So p divides every term in the sum

- Rearrange

$$|G| - \sum [G : C_G(x_i)] = |Z(G)|.$$

- p divides both terms on the LHS, so must divide the RHS, so $|Z(G)| \geq p$.

■

Proof (of b).
Strategy: examine $|G/Z(G)|$ by cases.

- 1: Then $G = Z(G)$ and G is abelian.
- p: Then $G/Z(G)$ is cyclic so G is abelian
- p^2: Not possible, since $|Z(G)| > 1$ by (a).

■

Proof (of c).

- By Sylow
  - $n_5 \mid 7^2, \quad n_5 \cong 1 \mod 5 \implies n_5 \in \{1, 7, 49\} \setminus \{7, 49\} = \{1\} \implies n_5 = 1$
  - $n_7 \mid 5^2, \quad n_7 \cong 1 \mod 7 \implies n_7 \in \{1, 5, 25\} \setminus \{5, 25\} = \{1\} \implies n_7 = 1$
- By recognition of direct products, $G = S_5 \times S_7$
  - By above, $S_5, S_7 \trianglelefteq G$
  - Check $S_5 \cap S_7 = \{e\}$ since they have coprime order.
  - Check $S_5 S_7 = G$ since $|S_5 S_7| = 5^2 7^2 = |G|$
- By (b), S_5, S_7 are abelian since they are groups of order p^2
- The direct product of abelian groups is abelian.

■

Proof (of d).

- $\mathbb{Z}_{5^2} \times \mathbb{Z}_{7^2}$
- $\mathbb{Z}_5^2 \times \mathbb{Z}_{7^2}$
- $\mathbb{Z}_{5^2} \times \mathbb{Z}_7^2$
- $\mathbb{Z}_5^2 \times \mathbb{Z}_7^2$

■

6 Groups: Simple and Solvable

6.1 ⋆ Fall 2016 #7

a. Define what it means for a group G to be *solvable*.

b. Show that every group G of order 36 is solvable.

Hint: you can use that S_4 is solvable.

6.2 Spring 2015 #4

Let N be a positive integer, and let G be a finite group of order N.

a. Let $\operatorname{Sym} G$ be the set of all bijections from $G \to G$ viewed as a group under composition. Note that $\operatorname{Sym} G \cong S_N$. Prove that the Cayley map

$$\begin{aligned} C : G &\to \operatorname{Sym} G \\ g &\mapsto (x \mapsto gx) \end{aligned}$$

is an injective homomorphism.

b. Let $\Phi : \operatorname{Sym} G \to S_N$ be an isomorphism. For $a \in G$ define $\varepsilon(a) \in \{\pm 1\}$ to be the sign of the permutation $\Phi(C(a))$. Suppose that a has order d. Prove that $\varepsilon(a) = -1 \iff d$ is even and N/d is odd.

c. Suppose $N > 2$ and $n \equiv 2 \bmod 4$. Prove that G is not simple.

Hint: use part (b).

6.3 Spring 2014 #1

Let p, n be integers such that p is prime and p does not divide n. Find a real number $k = k(p, n)$ such that for every integer $m \geq k$, every group of order $p^m n$ is not simple.

6.4 Fall 2013 #1

Let p, q be distinct primes.

a. Let $\bar{q} \in \mathbb{Z}_p$ be the class of $q \bmod p$ and let k denote the order of $\bar{q}$ as an element of $\mathbb{Z}_p^\times$. Prove that no group of order pq^k is simple.

b. Let G be a group of order pq, and prove that G is not simple.

6.5 Spring 2013 #4

Define a *simple group*. Prove that a group of order 56 can not be simple.

6.6 Fall 2019 Midterm #3 🚩

Show that there exist no simple groups of order 148.

7 Commutative Algebra

7.1 UFDs, PIDs, etc

7.1.1 Spring 2013 #2 ✨

a. Define a *Euclidean domain.*

b. Define a *unique factorization domain.*

c. Is a Euclidean domain an UFD? Give either a proof or a counterexample with justification.

d. Is a UFD a Euclidean domain? Give either a proof or a counterexample with justification.

Solution:

- R is Euclidean iff it admits a Euclidean algorithm: there is a degree function $f : R \to \mathbb{Z}_{\geq 0}$ such that for all $a, b \in R$, there exist $q, r \in R$ such that $a = bq + r$ where $f(r) < f(b)$ or $r = 0$.
- R is a UFD iff every $r \in R$ can be written as $r = u \prod_{i=1}^{n} p_i$ with $n \geq 0$, $u \in R^\times$, and p_i irreducible. This is unique up to associates of the p_i and reordering.
- Euclidean implies UFD:
  - Euclidean implies PID:
    - ◇ If $I \in \operatorname{Id}(R)$ one can use the degree function to find any $b \in I$ where $f(b)$ is minimal.
    - ◇ Then $I = \langle b \rangle$, since if $a \in I$ one can write $a = bq + r$ and use that $a - bq \in I \implies r \in I$.
    - ◇ But by minimality, we can't have $f(r) < f(b)$, so $r = 0$ and $a \mid b$, so $b \in \langle a \rangle$.
  - PID implies UFD:
    - ◇ Use that irreducible implies prime in a PID, so every $x \in R$ has some factorization into finitely many primes.
    - ◇ Supposing $x = u_p \prod_{i=1}^{m} p_i = u_q \prod_{i=1}^{n} q_i$, use that p_1 divides the LHS and so p_1

divides the RHS. WLOG, $p_1 \mid q_1$, so $q_1 = u_1 p_1$ for $u \in R^\times$, so $x = u_q u_1 p_1 \prod_{i=2}^m q_i$ by rewriting a term on the RHS.

◇ Note that this makes p_1, q_1 associates.

◇ Continuing up to m, we get

$$\begin{aligned} x &= u_p \prod_{i=1}^m p_i \\ &= u_q \prod_{i=1}^m u_i p_i \prod_{k=m+1}^n q_i \\ \implies u_p &= u_q \prod_{i=1}^m u_i \prod_{k=m+1}^n q_i \\ \tilde{u} &= \prod_{k=m+1}^n q_i, \end{aligned}$$

where we've moved all units to the LHS. This makes p_i, q_i associates for $i \leq m$.

◇ But primes aren't units and the product of nontrivial primes can't be a unit, so the right-hand side product must be empty.

◇ So $m = n$ and all p_i, q_i are associate, QED.

- UFD does not imply Euclidean:
  - It suffices to find a UFD that is not a PID.
  - Take $R := \mathbb{C}[x, y]$, which is a UFD by the usual factorization of polynomials. It is not a PID, since $\langle 2, x \rangle$ is not principal.

7.1.2 Fall 2017 #6 ✨

For a ring R, let $U(R)$ denote the multiplicative group of units in R. Recall that in an integral domain R, $r \in R$ is called *irreducible* if r is not a unit in R, and the only divisors of r have the form ru with u a unit in R.

We call a non-zero, non-unit $r \in R$ *prime* in R if $r \mid ab \implies r \mid a$ or $r \mid b$. Consider the ring $R = \{a + b\sqrt{-5} \mid a, b \in Z\}$.

a. Prove R is an integral domain.

b. Show $U(R) = \{\pm 1\}$.

c. Show $3, 2 + \sqrt{-5}$, and $2 - \sqrt{-5}$ are irreducible in R.

d. Show 3 is not prime in R.

e. Conclude R is not a PID.

Concepts Used:

- Integral domain: $ab = 0 \implies a \neq 0$ or $b \neq 0$.
- Prime: $p \mid ab \implies p \mid a$ or b.
- Reducible: $a = xy$ where x, y are proper divisors.
- Irreducible implies prime in a UFD.

Solution:

- R is an integral domain:
  - Let $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$ and set $\bar{\alpha}, \bar{\beta}$ be their conjugates.
  - Then
    $$0 = \alpha\beta = \alpha\bar{\alpha}\beta\bar{\beta} = (a^2 - 5b^2)(c^2 - 5d^2) \in \mathbb{Z},$$
    so one factor is zero.
  - If $a^2 = 5b^2$ then $a = \sqrt{5}b \notin \mathbb{Z}$ unless $a = b = 0$. Otherwise, the same argument forces $c = d = 0$.
- The units are ±1:
  - Use that $u \in R^\times \implies N(u) = \pm 1$, and $N(\alpha) = \alpha\bar{\alpha} = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2 = 1$ forces $b = 0$ and $a = \pm 1$.
- Irreducible elements:
  - $2, 3$ are irreducible because if (say) $3 = xy$ then $N(x)N(y) = N(3) = 9$, and if neither x, y are units then $N(x) = N(y) = 3$. But $N(a + b\sqrt{-5}) = a^2 + 5b^2$ and $a^2 + 5b^2 = 3$ has no solutions. The same argument works for 2.
  - $2 \pm \sqrt{-5}$ are irreducible because $N(2 + \sqrt{-5}) = 2^2 + 5(1) = 9$, and in fact $N(2 - \sqrt{-5}) = 2^2 + 5(-1)^2 = 9$. By the same argument as above, this forces irreducibility.
- 3 is not prime:
  - We can write $6 = (3)(2) = (1 + \sqrt{-5})(1 - \sqrt{-5})$, so if we assume 3 is prime we get $3 \mid (1 \pm \sqrt{-5})$.
  - But writing $(1 \pm \sqrt{-5}) = 3r$ for some $r \in R$ yields
    $$(1 \pm \sqrt{-5}) = 3(a + b\sqrt{-5}) \implies 3a = 1, 3b = \pm 1.$$
    These have no solutions $a, b \in \mathbb{Z}$. $\lightning$
- R is not a PID:
  - Use that irreducibles are prime in a UFD, which is not true here.

7.1.3 Spring 2017 #4 ✨

a. Let R be an integral domain with quotient field F. Suppose that $p(x), a(x), b(x)$ are monic polynomials in $F[x]$ with $p(x) = a(x)b(x)$ and with $p(x) \in R[x]$, $a(x)$ not in $R[x]$, and both $a(x), b(x)$ not constant.

Prove that R is not a UFD.

(You may assume Gauss' lemma)

b. Prove that $\mathbb{Z}[2\sqrt{2}]$ is not a UFD.

Hint: let $p(x) = x^2 - 2$.

Concepts Used:

- Gauss' lemma: for R a UFD with fraction field F, if f is reducible in $F[x]$ with $f = pq$ then there are $r, s \in R$ such that $f = (rp)(sq)$ reduces in $R[x]$.
- Corollary: R is a UFD iff $R[x]$ is a UFD.

Solution:

Proof (of 1).

- The important assumption is $a(x) \notin R[x]$, we'll assume R is a UFD and try to contradict this.
- Write $f(x) = a(x)b(x) \in F[x]$, then if R is a UFD we have $r, s \in F$ such that $f(x) = ra(x)sb(x) \in R[x]$.
- Since $a(x), b(x)$ are monic and $f = ab$, f is monic, and by the factorization in $R[x]$ we have $rs = 1$. So $r, s \in R^\times$.
- Then using that $ra(x) \in R[x]$, we have $r^{-1}ra(x) = a(x) \in R[x]$. ↯

■

Proof (of b).

- Set $R = \mathbb{Z}[2\sqrt{2}], F = \mathbb{Q}[2\sqrt{2}]$.
- Let $p(x) := x^2 - 2 \in R[x]$ which splits as $p(x) = (x + \sqrt{2})(x - \sqrt{2}) := a(x)b(x) \in F[x]$.
- Note neither $a(x), b(x)$ are in $R[x]$.
  - Explicitly, every monic linear $p \in R[x]$ is of the form $x + 2t\sqrt{2}$ with $t \in \mathbb{Z}$, and $\pm\sqrt{2} \neq 2t\sqrt{2}$ for any t.
- So we have $p(x) \in R[x]$ splitting as $p = ab$ in $F[x]$ with $a \notin R[x]$, so part (a) applies.

■

7.2 Ideals (Prime, Maximal, Proper, Principal, etc)

7.2.1 Fall 2013 #3 ✨

a. Define *prime ideal*, give an example of a nontrivial ideal in the ring $\mathbb{Z}$ that is not prime, and prove that it is not prime.

b. Define *maximal ideal*, give an example of a nontrivial maximal ideal in $\mathbb{Z}$ and prove that it is maximal.

Solution:

- $\mathfrak{p}$ is **prime** iff $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.
  - An ideal $I \trianglelefteq \mathbb{Z}$ that is not prime: $I := 8\mathbb{Z}$.
  - For example, $2 \cdot 4 \in 8\mathbb{Z}$ but neither 2 nor 4 is a multiple of 8.
- $\mathfrak{m}$ is **maximal** iff whenever $I \supseteq \mathfrak{m}$ is an ideal in R, then either $I = \mathfrak{m}$ or $I = R$.
  - A maximal ideal in $\mathbb{Z}$: $p\mathbb{Z}$. This is because primes are maximal in a PID and $p\mathbb{Z}$ is a prime ideal. Alternatively, "to contain is to divide" holds for Dedekind domains, so $m\mathbb{Z} \supseteq p\mathbb{Z} \iff m \mid p$, which forces $m = 1, p$, so either $m\mathbb{Z} = p\mathbb{Z}$ or $m\mathbb{Z} = \mathbb{Z}$.

7.2.2 Fall 2014 #8 🚩

Let R be a nonzero commutative ring without unit such that R does not contain a proper maximal ideal. Prove that for all $x \in R$, the ideal xR is proper.

You may assume the axiom of choice.

7.2.3 Fall 2014 #7 ✨

Give a careful proof that $\mathbb{C}[x, y]$ is not a PID.

Concepts Used:

- If $R[x]$ is a PID, then R is a field (not explicitly used).
- In $P := R[x_1, \cdots, x_n]$, there are degree functions $\deg_{x_n} : P \to \mathbb{Z}_{\geq 0}$.

Solution:

- The claim is that $I := \langle x, y \rangle$ is not principal.

- Toward a contradiction, if so, then $\langle x, y\rangle = \langle f\rangle$.
- So write $x = fg$ for some $g \in \mathbb{C}[x, y]$, then
  - $\deg_x(x) = 1$, so $\deg_x(fg) = 1$ which forces $\deg_x(f) \leq 1$.
  - $\deg_y(y) = 1$, so $\deg_y(fg) = 1$ which forces $\deg_y(f) \leq 1$.
  - So $f(x, y) = ax + by + c$ for some $a, b, c \in \mathbb{C}$.
  - $\deg_x(y) = 0$ and thus $\deg_x(fg) = 0$, forcing $a = 0$
  - $\deg_y(x) = 0$ and thus $\deg_y(fg) = 0$, forcing $b = 0$
  - So $f(x, y) = c \in \mathbb{C}$.
- But $\mathbb{C}[x]$ is a field, so c is a unit in $\mathbb{C}$ and thus $\mathbb{C}[x, y]$, so $\langle f\rangle = \langle c\rangle = \mathbb{C}[x, y]$.
- This is a contradiction, since $1 \not\in \langle x, y\rangle$:
  - Every element in $\alpha(x, y) \in \langle x, y\rangle$ is of the form $\alpha(x, y) = xp(x, y) + yq(x, y)$.
  - But $\deg_x(\alpha) \geq 1, \deg_y(\alpha) \geq 1$, while $\deg_x(1) = \deg_y(1) = 0$.
  - So $\langle x, y\rangle \neq \mathbb{C}[x, y]$.
- Alternatively, $\langle x, y\rangle$ is proper since $\mathbb{C}[x, y]/\langle x, y\rangle \cong \mathbb{C} \neq \mathbb{C}[x, y]$.

7.2.4 Spring 2019 #6 ✨

Let R be a commutative ring with 1.

Recall that $x \in R$ is nilpotent iff $xn = 0$ for some positive integer n.

a. Show that every proper ideal of R is contained within a maximal ideal.

b. Let $J(R)$ denote the intersection of all maximal ideals of R. Show that $x \in J(R) \iff 1 + rx$ is a unit for all $r \in R$.

c. Suppose now that R is finite. Show that in this case $J(R)$ consists precisely of the nilpotent elements in R.

Concepts Used:

- Definitions:

$$N(R) \coloneqq \left\{ x \in R \;\middle|\; x^n = 0 \text{ for some } n \right\}$$

$$J(R) \coloneqq \cap_{\mathfrak{m} \in \text{mSpec}} \mathfrak{m}.$$

- Zorn's lemma: if P is a poset in which every chain has an upper bound, P contains a maximal element.

Solution:

Proof (of a).
Define the set of proper ideals

$$S = \left\{ J \;\middle|\; I \subseteq J < R \right\},$$

which is a poset under set inclusion.
Given a chain $J_1 \subseteq \cdots$, there is an upper bound $J := \cup J_i$, so Zorn's lemma applies. ■

Proof (of b, $\implies$).
$\implies$:

- We will show that $x \in J(R) \implies 1 + x \in R^{\times}$, from which the result follows by letting $x = rx$.
- Let $x \in J(R)$, so it is in every maximal ideal, and suppose toward a contradiction that $1 + x$ is **not** a unit.
- Then consider $I = \langle 1 + x \rangle \trianglelefteq R$. Since $1+x$ is not a unit, we can't write $s(1+x) = 1$ for any $s \in R$, and so $1 \notin I$ and $I \neq R$
- So $I < R$ is proper and thus contained in some maximal proper ideal $\mathfrak{m} < R$ by part (1), and so we have $1 + x \in \mathfrak{m}$. Since $x \in J(R)$, $x \in \mathfrak{m}$ as well.
- But then $(1 + x) - x = 1 \in \mathfrak{m}$ which forces $\mathfrak{m} = R$.

■

Proof (of b, $\Longleftarrow$).
$\Longleftarrow$

- Fix $x \in R$, and suppose $1 + rx$ is a unit for all $r \in R$.
- Suppose towards a contradiction that there is a maximal ideal $\mathfrak{m}$ such that $x \notin \mathfrak{m}$ and thus $x \notin J(R)$.
- Consider
$$M' := \left\{ rx + m \;\middle|\; r \in R,\ m \in M \right\}.$$
- Since $\mathfrak{m}$ was maximal, $\mathfrak{m} \subsetneq M'$ and so $M' = R$.
- So every element in R can be written as $rx + m$ for some $r \in R, m \in M$. But $1 \in R$, so we have
$$1 = rx + m.$$
- So let $s = -r$ and write $1 = sx - m$, and so $m = 1 + sx$.
- Since $s \in R$ by assumption $1 + sx$ is a unit and thus $m \in \mathfrak{m}$ is a unit, a contradiction.
- So $x \in \mathfrak{m}$ for every $\mathfrak{m}$ and thus $x \in J(R)$.

■

Proof (of c: $J(R) = \mathfrak{N}(R)$).
$\mathfrak{N}(R) \subseteq J(R)$:

- Use the fact $x \in \mathfrak{N}(R) \implies x^n = 0 \implies 1 + rx$ is a unit $\iff x \in J(R)$ by (b):

$$\sum_{k=1}^{n-1} (-x)^k = \frac{1 - (-x)^n}{1 - (-x)} = (1+x)^{-1}.$$

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

- Let $x \in J(R) \setminus \mathfrak{N}(R)$.
- Since R is finite, $x^m = x$ for some $m > 0$.
- Without loss of generality, we can suppose $x^2 = x$ by replacing x^m with x^{2m}.
- If $1 - x$ is not a unit, then $\langle 1 - x \rangle$ is a nontrivial proper ideal, which by (a) is contained in some maximal ideal $\mathfrak{m}$. But then $x \in \mathfrak{m}$ and $1 - x \in \mathfrak{m} \implies x + (1 - x) = 1 \in \mathfrak{m}$, a contradiction.
- So $1 - x$ is a unit, so let $u = (1 - x)^{-1}$.
- Then

$$\begin{aligned}(1-x)x &= x - x^2 = x - x = 0 \\ &\implies u(1-x)x = x = 0 \\ &\implies x = 0.\end{aligned}$$

■

7.2.5 Spring 2018 #8 ✨

Let $R = C[0,1]$ be the ring of continuous real-valued functions on the interval $[0,1]$. Let I be an ideal of R.

a. Show that if $f \in I, a \in [0,1]$ are such that $f(a) \neq 0$, then there exists $g \in I$ such that $g(x) \geq 0$ for all $x \in [0,1]$, and $g(x) > 0$ for all x in some open neighborhood of a.

b. If $I \neq R$, show that the set $Z(I) = \left\{ x \in [0,1] \,\middle|\, f(x) = 0 \text{ for all } f \in I \right\}$ is nonempty.

c. Show that if I is maximal, then there exists $x_0 \in [0,1]$ such that $I = \left\{ f \in R \,\middle|\, f(x_0) = 0 \right\}$.

Remark 7.2.1: Cool problem, but pretty specific topological tricks needed.

Solution:

Proof (of a).

- Suppose $c := f(a) \neq 0$, noting that c may not be positive.
- By continuity, pick ε small enough so that $|x-a| < \varepsilon \implies |f(x) - f(a)| < c/2$. Since we're on the interval, we have $f(x) \in (f(a) - c/2, f(a) + c/2) = (c/2, 3c/2)$ which is a ball of radius $c/2$ about c, which thus doesn't intersect 0.
- So $f(x) \neq 0$ on this ball, and $g := f^2 > 0$ on it. Note that ideals are closed under products, so $g \in I$
- Moreover $f^2(x) \geq 0$ since squares are non-negative, so $g \geq 0$ on $[0,1]$.

■

Proof (of b).

- By contrapositive, suppose $V(I) = \emptyset$, we'll show I contains a unit and thus $I = R$.
- For each fixed $x \in [0,1]$, since $V(I)$ is empty there is some f_x such that $f_x(x) \neq 0$.
- By (a), there is some g_x with $g_x(x) > 0$ on a neighborhood $U_x \ni x$ and $g_x \geq 0$ everywhere.
- Ranging over all x yields a collection $\left\{(g_x, U_x) \;\middle|\; x \in [0,1]\right\}$ where $\{U_x\} \rightrightarrows [0,1]$.
- By compactness there is a finite subcover, yielding a finite collection $\{(g_k, U_k)\}_{k=1}^n$ for some n.
- Define the candidate unit as

$$G(x) := \frac{1}{\sum_{k=1}^n g_k(x)}.$$

- This is well-defined: fix an x, then the denominator is zero at x iff $g_k(x) = 0$ for all k. But since the U_k form an open cover, $x \in U_\ell$ for some ℓ, and $g_\ell > 0$ on U_ℓ.
- Since ideals are closed under sums, $H := \frac{1}{G} := \sum g_k \in I$. But H is clearly a unit since $HG = \mathrm{id}$.

■

Proof (of c).

- If $I \trianglelefteq R$ is maximal, $I \neq R$, and so by (b) we have $V(I) \neq \emptyset$.
- So there is some $x_0 \in [0,1]$ with $f(x_0) = 0$ for all $f \in I$.
- Define $\mathfrak{m}_{x_0} := \left\{f \in R \;\middle|\; f(x_0) = 0\right\}$, which is clearly an ideal.
  - This is a proper ideal, since constant nonzero functions are continuous and thus in R, not not $\mathfrak{m}_{x_0}$.
- We thus have $I \subseteq \mathfrak{m}_{x_0}$, and by maximality they are equal.

■

I'm not super convinced by c!

7.3 Zero Divisors and Nilpotents

7.3.1 Spring 2014 #5 ✨

Let R be a commutative ring and $a \in R$. Prove that a is not nilpotent $\iff$ there exists a commutative ring S and a ring homomorphism $\varphi : R \to S$ such that $\varphi(a)$ is a unit.

Note: by definition, a is nilpotent $\iff$ there is a natural number n such that $a^n = 0$.

Solution:
$\cancel{A} \implies \cancel{B}$:

- Suppose a is nilpotent, so $a^m = 0_R$, and suppose $\varphi : R \to S$ is a ring morphism.
- Ring morphisms send zero to zero, so $0_S = \varphi(0_R) = \varphi(a^m) = \varphi(a)^m$ and $\varphi(a)$ is nilpotent.
- But nontrivial rings can't contain nilpotent units: if u is a unit and $ut = 1$ with $u^k = 0$, then $1 = 1^k = (ut)^k = u^k t^k = 0$ and $R = 0$.

$A \implies B$:

- If a is not nilpotent, localize at the infinite multiplicative subset $A := \left\{1, a, a^2, \cdots\right\}$ to obtain $R\left[A^{-1}\right]$. Since $0 \not\in A$, this is not the zero ring.
- By the universal property, there is a map $\varphi : R \to R\left[A^{-1}\right]$, and the claim is that $\varphi(a)$ is a unit in $R\left[A^{-1}\right]$.
- More directly, $\varphi(a) = [a/1] \in \left\{p, q \;\middle|\; p \in R, q \in A\right\}$, which has inverse $[a/1]$.

7.3.2 Spring 2021 #5 ✨

Problem 7.3.1 (Spring 2021)
Suppose that $f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ is a zero divisor. Show that there is a nonzero $a \in \mathbb{Z}/n\mathbb{Z}$ with $af(x) = 0$.

Solution:

- Write $f(x) = \sum_{k=0}^{n} a_k x^k$, and supposing it's a zero divisor choose $g(x) = \sum_{k=0}^{m} b_k x^k$ of minimal degree so that $g \neq 0, b_m \neq 0$, and $f(x)g(x) = 0$.

- The claim is that the top coefficient b_m will suffice.
- Write the product:

$$0 = f(x)g(x) = (a_0 + \cdots + a_{n-1}x^{n-1} + a_n x^n)(b_0 + \cdots + b_{m-1}x^{m-1} + b_m x^m).$$

- Equating coefficients, the coefficient for x^{m+n} must be zero, so (**importantly**) $a_n b_m = 0$.
  - Since $a_n b_m = 0$, consider $a_n g(x)$. This has degree $d_1 \leq m-1$ but satisfies $a_n g(x) f(x) = a_n (g(x) f(x)) = 0$, so by minimality $a_n g(x) = 0$.
  - This forces $a_n b_0 = \cdots = a_n b_{m-1} = 0$, so a_n annihilates all of the b_k.
- Now consider the coefficient of x^{m+n-1}, given by $a_{n-1}b_m + a_n b_{m-1}$.
  - The second term $a_n b_{m-1} = 0$ since a_n annihilates all b_k, so (**importantly**) $a_{n-1}b_m = 0$.
  - Considering now $a_{n-1}g(x)$:
    - ◇ The same argument shows this has degree $d_2 \leq m-1$ but $a_{n-1}g(x)f(x) = 0$, so $a_{n-1}g(x) = 0$.
    - ◇ So a_{n-1} annihilates all b_k, and allowing this process to continue inductively.
- For good measure, the coefficient of x^{m+n-2} is $a_{n-2}b_m + a_{n-1}b_{m-1} + a_n b_{m-2}$.
  - Note that a_n, a_{n-1} annihilate all b_k, so (**importantly**) $a_{n-2}b_m = 0$, and so on.
- Thus $a_k b_m = 0$ for all $0 \leq k \leq n$, and by linearity and commutativity, we have

$$b_m f(x) = b_m \sum_{k=0}^{n} a_k x^k = \sum_{k=0}^{n} (b_m a_k) x^k = 0.$$

7.3.3 Fall 2018 #7 ✨

Let R be a commutative ring.

a. Let $r \in R$. Show that the map

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

is an R-module endomorphism of R.

b. We say that r is a **zero-divisor** if $r\bullet$ is not injective. Show that if r is a zero-divisor and $r \neq 0$, then the kernel and image of R each consist of zero-divisors.

c. Let $n \geq 2$ be an integer. Show: if R has exactly n zero-divisors, then $\#R \leq n^2$.

d. Show that up to isomorphism there are exactly two commutative rings R with precisely 2 zero-divisors.

You may use without proof the following fact: every ring of order 4 is isomorphic to exactly one of the following:

$$\frac{\mathbb{Z}}{4\mathbb{Z}}, \quad \frac{\frac{\mathbb{Z}}{2\mathbb{Z}}[t]}{(t^2+t+1)}, \quad \frac{\frac{\mathbb{Z}}{2\mathbb{Z}}[t]}{(t^2-t)}, \quad \frac{\frac{\mathbb{Z}}{2\mathbb{Z}}[t]}{(t^2)}.$$

Concepts Used:

- Testing module morphisms: $\varphi(sm+n) = s\varphi(m) + \varphi(n)$.
- First isomorphism theorem used for sizes: $R/\ker f \cong \operatorname{im} f$, so $\# R = \# \ker f \cdot \# \operatorname{im} f$.
- See 1964 Annals "Properties of rings with a finite number of zero divisors"

Solution:

Proof (of a).

- Let φ denote the map in question, it suffices to show that φ is R-linear, i.e. $\varphi(s\mathbf{x} + \mathbf{y}) = s\varphi(\mathbf{x}) + \varphi(\mathbf{y})$:

$$\begin{aligned}\varphi(s\mathbf{x}+\mathbf{y}) &= r(s\mathbf{x}+\mathbf{y}) \\ &= rs\mathbf{x} + r\mathbf{y} \\ &= s(r\mathbf{x}) + (r\mathbf{y}) \\ &= s\varphi(\mathbf{x}) + \varphi(\mathbf{y}).\end{aligned}$$

■

Proof (of b).
Let $\varphi_r(x) := rx$ be the multiplication map.

- Let $x \in \ker \varphi_r := \left\{ x \in R \;\middle|\; rx = 0 \right\}$.
- Since R is commutative $0 = rx = xr$, and so $r \in \ker \varphi_x$, so $\ker \varphi_x \neq 0$ and x is a zero divisor by definition.
- Let $y \in \operatorname{im} \varphi_r := \left\{ y := rx \;\middle|\; x \in R \right\}$, we want to show $\ker \varphi_y$ is nontrivial by producing some z such that $yz = 0$. Write $y := rx$ for some $x \in R$.
- Since r is a zero divisor, we can produce some $z \neq 0 \in \ker \varphi_r$, so $rz = 0$.
- Now using that R is commutative, we can compute

$$yz = (rx)z = (xr)z = x(rz) = x(0) = 0,$$

so $z \in \ker \varphi_y$.

■

Proof (of c).

- Let $Z := \{z_i\}_{i=1}^n$ be the set of n zero divisors in R.
- Let φ_i be the n maps $x \mapsto z_i x$, and let $K_i = \ker \varphi_i$ be the corresponding kernels.
- Fix an i.
- By (b), K_i consists of zero divisors, so

$$|K_i| \leq n < \infty \quad \text{for each } i.$$

- Now consider $R/K_i := \{r + K_i\}$.
- By the first isomorphism theorem, $R/K_i \cong \operatorname{im} \varphi$, and by (b) every element in the image is a zero divisor, so

$$[R : K_i] = |R/K_i| = |\operatorname{im} \varphi_i| \leq n.$$

- But then

$$|R| = [R : K_i] \cdot |K_i| \leq n \cdot n = n^2.$$

■

Proof (of d).

- By (c), if there are exactly 2 zero divisors then $|R| \leq 4$. Since every element in a finite ring is either a unit or a zero divisor, and $\left|R^{\times}\right| \geq 2$ since ± 1 are always units, we must have $|R| = 4$.
- Since the characteristic of a ring must divide its size, we have $\operatorname{ch} R = 2$ or 4.
- Using the hint, we see that only $\mathbb{Z}/(4)$ has characteristic 4, which has exactly 2 zero divisors given by $[0]_4$ and $[2]_4$.
- If R has characteristic 2, we can check the other 3 possibilities.
- We can write $\mathbb{Z}/(2)[t]/(t^2) = \left\{ a + bt \;\middle|\; a, b \in \mathbb{Z}/(2) \right\}$, and checking the multiplication table we have

$$\begin{array}{c|cccc} & 0 & 1 & t & 1+t \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & t & 1+t \\ t & 0 & t & \mathbf{0} & t \\ 1+t & 0 & 1+t & t & 1 \end{array},$$

  and so we find that $t, 0$ are the zero divisors.
- In $\mathbb{Z}/(2)[t]/(t^2 - t)$, we can check that $t^2 = t \implies tt^2 = t^2 \implies t(t^2+1) = 0 \implies t(t+1) = 0$, so both t and $t+1$ are zero divisors, along with zero, so this is not a possibility.
- Similarly, in $\mathbb{Z}/(2)[t]/(t^2 + t + 1)$, we can check the bottom-right corner of the multiplication table to find

$$\begin{bmatrix} \begin{array}{c|cc} & t & 1+t \\ \hline t & 1+t & 1 \\ t & 1 & t \end{array} \end{bmatrix},$$

  and so this ring only has one zero divisor.
- Thus the only possibilities are:

$$\begin{aligned} R &\cong \mathbb{Z}/(4) \\ R &\cong \mathbb{Z}/(2)[t]/(t^2). \end{aligned}$$

■

7.4 Zorn's Lemma

7.4.1 Fall 2013 #4 🚩

Let R be a commutative ring with $1 \neq 0$. Recall that $x \in R$ is *nilpotent* iff $x^n = 0$ for some positive integer n.

a. Show that the collection of nilpotent elements in R forms an ideal.

b. Show that if x is nilpotent, then x is contained in every prime ideal of R.

c. Suppose $x \in R$ is not nilpotent and let $S = \left\{ x^n \,\middle|\, n \in \mathbb{N} \right\}$. There is at least on ideal of R disjoint from S, namely (0).

   By Zorn's lemma the set of ideals disjoint from S has a maximal element with respect to inclusion, say I. In other words, I is disjoint from S and if J is any ideal disjoint from S with $I \subseteq J \subseteq R$ then $J = I$ or $J = R$.

   Show that I is a prime ideal.

d. Deduce from (a) and (b) that the set of nilpotent elements of R is the intersection of all prime ideals of R.

7.4.2 Fall 2015 #3 ✨

Let R be a rng (a ring without 1) which contains an element u such that for all $y \in R$, there exists an $x \in R$ such that $xu = y$.

Prove that R contains a maximal left ideal.

Hint: imitate the proof (using Zorn's lemma) in the case where R does have a 1.

Solution:

- Define the map

$$\begin{aligned} \varphi_u : R &\to R \\ x &\mapsto xu, \end{aligned}$$

  which is right-multiplication by u. By assumption, φ_u is surjective, so the principal ideal Ru equals R.

- Then $K := \ker \varphi_u \in \operatorname{Id}(R)$ is an ideal.

- K is proper – otherwise, noting $Ru = R$, if $K = R$ we have $Ru = 0$ and thus $R = 0$. So suppose $R \neq 0$.

- Take a poset $S := \left\{ J \in \operatorname{Id}(R) \;\middle|\; J \supseteq K, J \neq R \right\}$, the set of all ideals containing K, ordered by subset inclusion. Note that $K \in S$, so S is nonempty.

- Apply Zorn's lemma: let $C : C_1 \subseteq C_2 \subseteq \cdots$ be a chain (totally ordered sub-poset) in S. If C is the empty chain, K is an upper bound. Otherwise, if C is nonempty, define $\widehat{C} := \bigcup_{i=1}^{\infty} C_i$.
  - $\widehat{C}$ is an ideal: if $a, b \in \widehat{C}$, then $a \in C_i, b \in C_j$ for some i, j. But without loss of generality, using that chains are totally ordered, $C_i \subseteq C_j$, so $a, b \in C_j$ and thus $ab \in C_j$. Similarly for $x \in \widehat{C}$, $x \in C_j$ for some j, and thus $Rx \subseteq C_j$ since C_j is an ideal.
  - $\widehat{C}$ is in S: It clearly contains K, since for example $K \subseteq C_1 \subseteq \widehat{C}$.
    - ◇ That $\widehat{C} \neq R$: an ideal equals R iff it contains a unit. But if $r \in \widehat{C}$ is a unit, $r \in C_j$ for some j is a unit, making $C_j = R$. ↯

- So by Zorn's lemma, $\widehat{C}$ contains a maximal ideal (incidentally containing K).

7.4.3 Spring 2015 #7 ✨

Let R be a commutative ring, and $S \subset R$ be a nonempty subset that does not contain 0 such that for all $x, y \in S$ we have $xy \in S$. Let $\mathcal{I}$ be the set of all ideals $I \trianglelefteq R$ such that $I \cap S = \emptyset$.

Show that for every ideal $I \in \mathcal{I}$, there is an ideal $J \in \mathcal{I}$ such that $I \subset J$ and J is not properly contained in any other ideal in $\mathcal{I}$.

Prove that every such ideal J is prime.

Solution:

- Restating, take the poset $S := \left\{ J \in \operatorname{Id}(R) \;\middle|\; J \cap S = \emptyset, I \neq R, I \subseteq J \right\}$ ordered by inclusion. Note that S is nonempty since it contains I. It suffices to produce a maximal element of S.
- Applying Zorn's lemma, let $C : C_1 \subseteq C_2 \subseteq \cdots$ be a chain and define $\widehat{C} := \cup C_i$.
- By standard arguments, $\widehat{C} \in \operatorname{Id}(R)$ and $\widehat{C} \supseteq I$, and it suffices to show $\widehat{C} \cap S = \emptyset$ and $\widehat{C} \neq R$.
- $\widehat{C} \cap S = \emptyset$:
  - By contradiction, if $x \in \widehat{C} \cap S$ then $x \in C_j$ for some j, and $x \in S$. But then $x \in C_j \cap S = \emptyset$.
- $\widehat{C} \neq R$:
  - By contradiction, if so then $1 \in \widehat{C} \implies 1 \in C_j$ for some j, forcing $C_j = R$.
- So Zorn's lemma applies and we obtain some ideal $\mathfrak{p}$, which we now claim is prime.
- Let $ab \in \mathfrak{p}$, we want to show $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

- Suppose not, then neither $a, b \in \mathfrak{p}$. By maximality, $\mathfrak{p} + Ra = R$, and so $\mathfrak{p} + Ra$ intersects S. Similarly $\mathfrak{p} + Rb = R$ so $\mathfrak{p} + Rb$ intersects S.
- Produce elements $x := p_1 + r_1 a, y := p_2 + r_2 b \in S$, then since S is multiplicatively closed,

$$\begin{aligned} xy &:= (p_1 + r_1 a)(p_2 + r_2 b) \in S \\ \implies & p_1 p_2 + p_1 r_2 b + p_2 r_1 a + r_1 r_2 ab \in S \\ \implies & xy \in \mathfrak{p} + \mathfrak{p}Rb + \mathfrak{p}Ra + R\mathfrak{p} && \text{since } p_i, ab \in \mathfrak{p} \\ \implies & xy \in (\mathfrak{p} + Rb + Ra + R)\mathfrak{p} \subseteq \mathfrak{p}. \end{aligned}$$

But then $xy \in S \cap \mathfrak{p}$, a contradiction.

7.4.4 Spring 2013 #1 ✨

Let R be a commutative ring.

a. Define a *maximal ideal* and prove that R has a maximal ideal.

b. Show than an element $r \in R$ is not invertible $\iff$ r is contained in a maximal ideal.

c. Let M be an R-module, and recall that for $0 \neq \mu \in M$, the *annihilator* of μ is the set

$$\operatorname{Ann}(\mu) = \left\{ r \in R \;\middle|\; r\mu = 0 \right\}.$$

Suppose that I is an ideal in R which is maximal with respect to the property that there exists an element $\mu \in M$ such that $I = \operatorname{Ann}(\mu)$ for some $\mu \in M$. In other words, $I = \operatorname{Ann}(\mu)$ but there does not exist $\nu \in M$ with $J = \operatorname{Ann}(\nu) \subsetneq R$ such that $I \subsetneq J$.

Prove that I is a prime ideal.

Solution:

Proof (part a and b).

- Maximal: a proper ideal $I \trianglelefteq R$, so $I \neq R$, such that if $J \supseteq I$ is any other ideal, $J = R$.
- Existence of a maximal ideal: use that $0 \in \operatorname{Id}(R)$ always, so $S := \left\{ I \in \operatorname{Id}(R) \;\middle|\; I \neq R \right\}$ is a nonempty poset under subset inclusion. Applying the usual Zorn's lemma argument produces a maximal element.

■

Proof (part c).
$\Longleftarrow$: By contrapositive: if $r \in R$ is a unit and $\mathfrak{m}$ is maximal, then $r \in \mathfrak{m} \implies \mathfrak{m} = R$, contradicting that $\mathfrak{m}$ is proper.
$\implies$:

- Suppose a is not a unit, we'll produce a maximal ideal containing it.
- Let $I := Ra$ be the principal ideal generated by a, then $Ra \neq R$ since a is not a unit.
- Take a poset $S := \left\{ J \in \operatorname{Id}(R) \;\middle|\; J \supseteq Ra, J \neq R \right\}$ ordered by set inclusion.
  - Let C_* be a chain in S, set $\widehat{C} := \cup C_i$. Then $\widehat{C} \in S$:
    - ◇ $\widehat{C} \neq R$, since if so it contains a unit, forcing some C_i to contain a unit and thus equal R.
    - ◇ $\widehat{C} \supseteq Ra$, since e.g. $\widehat{C} \supseteq C_1 \supseteq Ra$.
    - ◇ $\widehat{C}$ is an ideal since $xy \in \widehat{C} \implies x \in C_i, y \in C_j$ and $C_i \subseteq C_j$ without loss of generality, so $xy \in C_j \subseteq \widehat{C}$.
- Then $Ra \subseteq \widehat{C}$, some maximal ideal.

■

Proof (of d).

- Write $I := \operatorname{Ann}(u)$ for some u, and toward a contradiction suppose $ab \in I$ but $a, b \notin I$.
- Then $abu = 0$ but $au \neq 0, bu \neq 0$.
- Since $abu = 0$, we have $a \in \operatorname{Ann}(bu)$. Note that $\operatorname{Ann}(bu) \supseteq \operatorname{Ann}(u)$, since $su = 0 \implies bsu = sbu = 0$.
- We can't have $\operatorname{Ann}(bu) = R$, since if $sbu = 0$ for all $s \in R$, so we could take $s = 1$ to get $bu = 0$ and $b \in \operatorname{Ann}(u)$.
- By maximality, this forces $\operatorname{Ann}(u) = \operatorname{Ann}(bu)$, so $sbu = 0 \implies su = 0$ for any $s \in R$.
- Now take $s = a$, and since $abu = 0$ we get $au = 0$ and $a \in \operatorname{Ann}(u)$. $\lightning$

■

7.4.5 Fall 2019 #6 ✨

Let R be a commutative ring with multiplicative identity. Assume Zorn's Lemma.

a. Show that

$$N = \left\{ r \in R \;\middle|\; r^n = 0 \text{ for some } n > 0 \right\}$$

is an ideal which is contained in any prime ideal.

b. Let r be an element of R not in N. Let S be the collection of all proper ideals of R not containing any positive power of r. Use Zorn's Lemma to prove that there is a prime ideal in S.

c. Suppose that R has exactly one prime ideal P . Prove that every element r of R is either nilpotent or a unit.

Concepts Used:

- Prime ideal: $\mathfrak{p}$ is prime iff $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- Silly fact: 0 is in every ideal!
- **Zorn's Lemma:** Given a poset, if every chain has an upper bound, then there is a maximal element. (Chain: totally ordered subset.)
- **Corollary:** If $S \subset R$ is multiplicatively closed with $0 \notin S$ then $\left\{I \trianglelefteq R \;\middle|\; J \cap S = \emptyset\right\}$ has a maximal element.

  Prove this
- **Theorem:** If R is commutative, maximal $\implies$ prime for ideals.

  Prove this
- **Theorem:** Non-units are contained in a maximal ideal. (See HW?)

Solution:

Proof (of a).

- Let $\mathfrak{p}$ be prime and $x \in N$.
- Then $x^k = 0 \in \mathfrak{p}$ for some k, and thus $x^k = xx^{k-1} \in \mathfrak{p}$.
- Since $\mathfrak{p}$ is prime, inductively we obtain $x \in \mathfrak{p}$.

■

Proof (of b).

- Let $S = \left\{r^k \;\middle|\; k \in \mathbb{N}\right\}$ be the set of positive powers of r.
- Then $S^2 \subseteq S$, since $r^{k_1}r^{k_2} = r^{k_1+k_2}$ is also a positive power of r, and $0 \notin S$ since $r \neq 0$ and $r \notin N$.
- By the corollary, $\left\{I \trianglelefteq R \;\middle|\; I \cap S = \emptyset\right\}$ has a maximal element $\mathfrak{p}$.
- Since R is commutative, $\mathfrak{p}$ is prime.

■

Proof (of c).

- Suppose R has a unique prime ideal $\mathfrak{p}$.
- Suppose $r \in R$ is not a unit, and toward a contradiction, suppose that r is also not nilpotent.
- Since r is not a unit, r is contained in some maximal (and thus prime) ideal, and thus $r \in \mathfrak{p}$.
- Since $r \notin N$, by (b) there is a maximal ideal $\mathfrak{m}$ that avoids all positive powers of r. Since $\mathfrak{m}$ is prime, we must have $\mathfrak{m} = \mathfrak{p}$. But then $r \notin \mathfrak{p}$, a contradiction.

■

7.5 Noetherian Rings

7.5.1 Fall 2015 #4 ✨

Let R be a PID and $(a_1) < (a_2) < \cdots$ be an ascending chain of ideals in R. Prove that for some n, we have $(a_j) = (a_n)$ for all $j \geq n$.

Solution:

- Let $I := \cup Ra_i$ which is an ideal in a PID and thus $I = Rb$ for some b.
- Using that $b \in I$, which is a union, we have $Rb \in Ra_m$ for some m.
- Thus $I = R_b \subseteq Ra_m$, and $Ra_m \subseteq I$ by definition of I, so $Rb = Ra_m$.
- In particular, since $Ra_m \subseteq Ra_{m+1}$ by assumption, and $Ra_{m+1} \subseteq Rb \subseteq Ra_m$ since $Rb = I$, we have $Ra_m = Ra_{m+1}$. So inductively, the chain stabilizes at m.

7.5.2 Spring 2021 #6 🚩

a. Carefully state the definition of **Noetherian** for a commutative ring R.

b. Let R be a subset of $\mathbb{Z}[x]$ consisting of all polynomials

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

such that a_k is even for $1 \leq k \leq n$. Show that R is a subring of $\mathbb{Z}[x]$.

c. Show that R is not Noetherian.

Hint: consider the ideal generated by $\left\{ 2x^k \;\middle|\; 1 \leq k \in \mathbb{Z} \right\}$.

Solution:

- A ring is **Noetherian** iff R satisfies the ascending chain condition: every chain of ideals $A_1 \subseteq A_2 \subseteq \cdots$ eventually stabilizes, so $A_m \subseteq A_{m+1} = A_{m+2} = \cdots$.
- That R is a subring of $\mathbb{Z}[x]$:
  - $(R, +)$ is an abelian subgroup: note that $f(x) + g(x) = \sum a_k x^k + \sum b_k x^k = \sum (a_k + b_k) x^k$, so if a_k, b_k are even then $a_k + b_k$ is even. It's closed under inverses, since a_k is even iff $-a_k$ is even, and contains zero.
  - $(R, \cdot)$ is a submonoid: $f(x)g(x) = \sum_{n=1}^{N} \left(\sum_{k=1}^{n} a_k b_{n-k} \right) x^k$ where without loss of generality, $\deg f = \deg g = n$ by setting coefficients to zero. Then sums and products of even integers are even, so $fg \in R$.
- That R is not Noetherian: it suffices to show that R contains an ideal that is not finitely generated.
- The claim is that setting $S := \left\{ 2x^k \right\}_{k \in \mathbb{Z}_{\geq 1}}$ and taking

$$I := \langle S \rangle = \sum_{k \in \mathbb{Z}_{\geq 1}} R \cdot 2x^k := \left\{ \sum_{i=1}^{m} r_k(x) 2x^k \;\middle|\; r_k(x) \in 2\mathbb{Z}[x], m \in \mathbb{Z}_{\geq 0} \right\}$$

  yields an ideal that is not finitely generated.
- Suppose toward a contradiction that $\{g_1, g_2, \cdots, g_M\}$ were a finite generating set, where each $g_i \in I$.

???

7.6 Simple Rings

7.6.1 Fall 2017 #5 ✨

A ring R is called *simple* if its only two-sided ideals are 0 and R.

a. Suppose R is a commutative ring with 1. Prove R is simple if and only if R is a field.

b. Let k be a field. Show the ring $M_n(k)$, $n \times n$ matrices with entries in k, is a simple ring.

Concepts Used:

- Nonzero proper ideals contain at least one nonzero element.
- $I = R$ when $1 \in I$.

- Effects of special matrices: let A_{ij} be a matrix with only a 1 in the ij position.
  - Left-multiplying $A_{ij}M$ moves row j to row i and zeros out the rest of M.
  - Right-multiplying MA_{ij} moves column i to column j and zeros out the rest.
  - So $A_{ij}MA_{kl}$ moves entry j,k to i,l and zeros out the rest.

Solution:

Proof (of a).
$\implies$:

- Suppose $\operatorname{Id}(R) = \{\langle 0 \rangle, \langle 1 \rangle\}$. Then for any nonzero $r \in R$, the ideal $\langle r \rangle = \langle 1 \rangle$ is the entire ring.
- In particular, $1 \in \langle r \rangle$, so we can write $a = tr$ for some $t \in R$.
- But then $r \in R^\times$ with $t \coloneqq r^{-1}$.

$\impliedby$:

- Suppose R is a field and $I \in \operatorname{Id}(R)$ is an ideal.
- If $I \neq \langle 0 \rangle$ is proper and nontrivial, then I contains at least one nonzero element $a \in I$.
- Since R is a field, $a^{-1} \in R$, and $aa^{-1} = 1 \in I$ forces $I = \langle 1 \rangle$.

■

Proof (of b).
- Let $J \trianglelefteq R$ be a nonzero two-sided ideal, noting that R is noncommutative – the claim is that J contains I_n, the $n \times n$ identity matrix, and thus $J = R$.
- Pick a nonzero element $M \in I$, then M has a nonzero entry mij.
- Let A_{ij} be the matrix with a 1 in the i,j position and zeros elsewhere.
  - Left-multiplying $A_{ij}M$ moves row j to row i and zeros out the rest of M.
  - Right-multiplying MA_{ij} moves column i to column j and zeros out the rest.
  - So $A_{ij}MA_{kl}$ moves entry j,k to i,l and zeros out the rest.
- So define $B \coloneqq A_{i,i}MA_{j,i}$, which movies m_{ij} to the i,i position on the diagonal and has zeros elsewhere.
- Then $m_{ij}^{-1}\varepsilon_{ii} \coloneqq A_{ii}$ is a matrix with 1 in the i,i spot for any i. Since I is an ideal, we have $\varepsilon_{ii} \in I$ for every i.
- We can write the identity I_n as $\displaystyle\sum_{i=1}^n \varepsilon_{ii}$, so $I_n \in I$ and $I = R$.

■

7.6.2 Spring 2016 #8 ✨

Let R be a simple rng (a nonzero ring which is not assume to have a 1, whose only two-sided ideals are (0) and R) satisfying the following two conditions:

i. R has no zero divisors, and
ii. If $x \in R$ with $x \neq 0$ then $2x \neq 0$, where $2x \coloneqq x + x$.

Prove the following:

a. For each $x \in R$ there is one and only one element $y \in R$ such that $x = 2y$.

b. Suppose $x, y \in R$ such that $x \neq 0$ and $2(xy) = x$, then $yz = zy$ for all $z \in R$.

You can get partial credit for (b) by showing it in the case R has a 1.

Remark 7.6.1: A general opinion is that this is not a great qual problem! Possibly worth skipping.

Concepts Used:

- R has no left zero divisors iff R has the left cancellation property: $xa = xb \implies a = b$.
- R has no right zero divisors iff R has the right cancellation property: $ax = bx \implies a = b$.

Solution:
Note: solutions borrowed from folks on Math twitter!

Proof (part 1).

- Existence: the claim is that $2R := \left\{ 2y \;\middle|\; y \in R \right\}$ is a nontrivial two-sided ideal of R, forcing $2R = R$ by simpleness.
  - That $2R \neq 0$ follows from condition (1): Provided $y \neq 0$, we have $2y \neq 0$, and so if $R \neq 0$ then there exists some nonzero $a \in R$, in which case $2a \neq 0$ and $2a \in 2R$.
  - That $2R$ is a right ideal: clear, since $(2y) \cdot r = 2(yr) \in 2R$.
  - That $2R$ is a left ideal: use that multiplication is distributive:

$$r \cdot 2y := r(y+y) = ry + ry := 2(ry) \in 2R.$$

- So $2R = R$ by simpleness.
- Uniqueness:
  - Use the contrapositive of condition (1), so that $2x = 0 \implies x = 0$.
  - Suppose toward a contradiction that $x = 2y_1 = 2y_2$, then

$$0 = x - x = 2y_1 - 2y_2 = 2(y_1 - y_2) \implies y_1 - y_2 = 0 \implies y_1 = y_2.$$

■

Proof (part 2).

- First we'll show $z = 2(yz)$:

$$\begin{aligned} xy + xy &= x \\ \implies xy + xy - x &= 0 \\ \implies xyz + xyz - xz &= 0 \\ \implies x(yz + yz - z) &= 0 \\ \implies yz + yz - z &= 0 && \text{since } x \neq 0 \text{ and no zero divisors} \\ \implies 2(yz) &= z. \end{aligned}$$

- Now we'll show $z = 2(zy)$:

$$\begin{aligned} yz + yz &= z \\ \implies zyz + zyz &= zz \\ \implies zyz + zyz - zz &= 0 \\ \implies (zy + zy - z)z &= 0 \\ \implies z = 0 \text{ or } zy + zy - z &= 0 && \text{no zero divisors .} \end{aligned}$$

- Then if $z = 0$, we have $yz = 0 = zy$ and we're done.
- Otherwise, $2(zy) = z$, and thus

$$2(zy) = z = 2(yz) \implies 2(zy - yz) = 0 \implies zy - yz = 0,$$

so $zy = yz$.

■

Proof (of 2, if R is unital).

- If $1 \in R$,

$$\begin{aligned} 2xy &= x \\ \implies 2xy - x &= 0 \\ \implies x(2y-1) &= 0 \\ \implies 2y - 1 &= 0 && x \neq 0 \text{ and no zero divisors} \\ \implies 2y &= 1. \end{aligned}$$

- Now use

$$\begin{aligned} 1 \cdot z &= z \cdot 1 \\ \implies (2y)z &= z(2y) \\ \implies (y+y)z &= z(y+y) \\ \implies yz + yz &= zy + zy \\ \implies 2(yz) &= 2(zy) \\ \implies 2(yz - zy) &= 0 \\ \implies yz - zy &= 0 \end{aligned}$$

$$,$$

  using condition (2).

■

7.7 Unsorted

7.7.1 Fall 2019 #3 ✨

Let R be a ring with the property that for every $a \in R, a^2 = a$.

a. Prove that R has characteristic 2.

b. Prove that R is commutative.

Strategy:

- Just fiddle with direct computations.
- Context hint: that we should be considering things like x^2 and $a+b$.

Solution:

Proof (of a).

$$2a = (2a)^2 = 4a^2 = 4a \implies 2a = 0.$$

Note that this implies $x = -x$ for all $x \in R$. ■

Proof (of b).

$$\begin{aligned} a + b = (a+b)^2 = a^2 + ab + ba + b^2 &= a + ab + ba + b \\ &\implies ab + ba = 0 \\ &\implies ab = -ba \\ &\implies ab = ba \quad \text{by (a)}. \end{aligned}$$

■

7.7.2 Spring 2018 #5 ✨

Let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad N = \begin{pmatrix} x & u \\ -y & -v \end{pmatrix}$$

over a commutative ring R, where b and x are units of R. Prove that

$$MN = \begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix} \implies MN = 0.$$

Solution:

- Multiply everything out to get
$$\begin{bmatrix} ax - by & au - bv \\ cx - dy & cu - dv \end{bmatrix},$$
so it suffices to show $cu = dv$ given
$$\begin{aligned} ax &= by \\ cx &= dy \\ au &= bv. \end{aligned}$$
- Writing cu:

  - Use that $b \in R^\times$, left-multiply (1) by b^{-1} to get $b^{-1}ax = y$
  - Substitute y into (2) to get $cx = d(b^{-1}ax)$.
  - Since $x \in R^\times$, right-multiply by x^{-1} to get $c = db^{-1}a$ and thus $cu = db^{-1}au$.
  - Summary:

$$\begin{aligned} ax = by &\implies b^{-1}ax = y \\ &\implies cx = dy = d(b^{-1}ax) \\ &\implies c = db^{-1}a \\ &\implies cu = db^{-1}au. \end{aligned}$$

- Writing dv:
  - Left-multiply (3) by b^{-1} to get $b^{-1}au = v$.
  - Left-multiply by d to get $db^{-1}au = dv$
  - Summary:

$$\begin{aligned} au = bv &\implies b^{-1}au = v \\ &\implies db^{-1}au = dv. \end{aligned}$$

- So

$$cu = db^{-1}au = dv.$$

7.7.3 Spring 2014 #6 🚩

R be a commutative ring with identity and let n be a positive integer.

a. Prove that every surjective R-linear endomorphism $T : R^n \to R^n$ is injective.

b. Show that an injective R-linear endomorphism of R^n need not be surjective.

8 | Galois Theory

8.1 General Galois Extensions

8.1.1 Fall 2020 #4 ✨

Let K be a Galois extension of F, and let $F \subset E \subset K$ be inclusions of fields. Let $G := \mathsf{Gal}(K/F)$ and $H := \mathsf{Gal}(K/E)$, and suppose H contains $N_G(P)$, where P is a Sylow p-subgroup of G for p a prime. Prove that $[E : F] \equiv 1 \bmod p$.

Concepts Used:
The correspondence:

$$\begin{tikzcd}
K & & 1 \arrow[d, hook, "{[H:1]}"'] \arrow[dd, bend left, "{[G:1]}"] \\
E \arrow[u, hook, "{[K:E]}"] & {} \arrow[r, Rightarrow, "\mathsf{Gal}(K/-)"'] & H := \mathsf{Gal}(K/E) \arrow[d, hook, "{[G:H]}"'] \\
F \arrow[u, hook, "{[E:F]}"] \arrow[uu, bend right, "{[K:F]}"'] & & G := \mathsf{Gal}(K/F)
\end{tikzcd}$$

Link to Diagram

Normalizers:

$$N_G(P) = \left\{ g \in G \;\middle|\; gPg^{-1} = P \right\}.$$

Solution:

- Reduce to a group theory problem: $[E:F] = [G:H]$, despite the fact that E/F is not necessarily Galois. This is because we can count in towers:

$$\begin{aligned}
[K:F] = [K:E][E:F] &\implies [G:1] = [K:E][H:1] \\
&\implies \#G = [K:E]\#H \\
&\implies [G:H] = \frac{\#G}{\#H} = [K:E].
\end{aligned}$$

- Essential fact: if $P \in \mathrm{Syl}_p(G)$, we can use that $P \subseteq N_G(P) \subset H$ and so $P \in \mathrm{Syl}_p(H)$ as well.
- Now use that $N_G(P) \subseteq H$, and do Sylow theory for P in both G and H:
  - Sylow 3 on G yields $n_p(G) = [G : N_G(P)] \equiv 1 \bmod p$.
  - Sylow 3 on H yields $n_p(H) = [G : N_H(P)] \equiv 1 \bmod p$.
- Claim: $N_H(P) = N_G(P)$.
  - We have $N_H(P) \subseteq N_G(P)$ since $H \subseteq G$, so $hPh^{-1} = P$ remains true regarding either $h \in H$ or $h \in G$.
  - For $N_G(P) \subseteq N_H(P)$, use that $N_G(P) \subseteq H$ and so $gPg^{-1} = P$ implies $g \in H$, so $g \in N_H(P)$.
- Now morally one might want to apply an isomorphism theorem:

$$\frac{G/N_G(P)}{H/N_H(P)} = \frac{G/N_H(P)}{H/N_H(P)} \cong \frac{G}{H},$$

but we don't have normality. However, we can still get away with the corresponding counting argument if everything is finite:

$$\frac{[G : N_G(P)]}{[H : N_H(P)]} = \frac{[G : N_H(P)]}{[H : N_H(P)]} = \frac{\#G/\#N_H(P)}{\#H/\#N_H(P)} = \frac{\#G}{\#H} = [G : H].$$

- We have an equation of the form $n_p(G)/n_p(H) = m$, and we want to show $m \equiv 1 \mod p$. So write

$$\begin{aligned}
\frac{n_p(G)}{n_p(H)} = m &\implies mn_p(H) = n_p(G) \\
&\implies mn_p(H) \equiv n_p(G) \mod p \\
&\implies m \cdot 1 \equiv 1 \mod p \\
&\implies m \equiv 1 \mod p.
\end{aligned}$$

8.1.2 Fall 2019 Midterm #9 ✨

Let $n \geq 3$ and ζ_n be a primitive nth root of unity. Show that $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \varphi(n)/2$ for φ the totient function.

Solution:

- Some notation: let $\alpha_k \coloneqq \zeta_n^k + \zeta_n^{-k}$.
- Let $m(x)$ be the minimal polynomial of $\alpha_1 \coloneqq \zeta_n + \zeta_n^{-1}$. Note that $\alpha_1 \in \mathbb{Q}(\zeta_n)$.
- Use that $\mathsf{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong C_n^\times$, consisting of maps $\sigma_k : \zeta \mapsto \zeta^k$ for $\gcd(k, n) = 1$, of which there are $\varphi(n)$ many.
- Galois transitively permutes the roots of irreducible polynomials, so the roots of m are precisely the Galois conjugates of α, i.e. the Galois orbit of α, so we can just compute it. For illustrative purposes, suppose n is prime, then

$$\begin{aligned}
\sigma_1(\zeta_n + \zeta_n^{-1}) &= \zeta_n + \zeta_n^{-1} = \alpha_1 \\
\sigma_2(\zeta_n + \zeta_n^{-1}) &= \zeta_n^2 + \zeta_n^{-2} = \alpha_2 \\
\sigma_3(\zeta_n + \zeta_n^{-1}) &= \zeta_n^3 + \zeta_n^{-3} = \alpha_3 \\
&\vdots \\
\sigma_{n-1}(\zeta_n + \zeta_n^{-1}) &= \zeta_n^{n-1} + \zeta_n^{-(n-1)} = \zeta_n^{-1} + \zeta_n^{1} = \alpha_1 \\
\sigma_{n-2}(\zeta_n + \zeta_n^{-1}) &= \zeta_n^{n-2} + \zeta_n^{-(n-2)} = \zeta_n^{-2} + \zeta_n^{2} = \alpha_2 \\
\sigma_{n-3}(\zeta_n + \zeta_n^{-1}) &= \zeta_n^{n-3} + \zeta_n^{-(n-3)} = \zeta_n^{-3} + \zeta_n^{3} = \alpha_3,
\end{aligned}$$

where we've used that $\zeta^k = \zeta^{k \mod n}$. From this, we see that $\sigma_k(\alpha_1) = \sigma_{n-k}(\alpha_1)$ and we pick up $(n-1)/2$ distinct conjugates.

- For n not prime, the exact same argument runs through $\varphi(n)$ values of k for σ_k, and again yields $\sigma_k(\alpha_1) = \sigma_{\varphi(n)-k}(\alpha_1)$. Matching them up appropriately yields $\varphi(n)/2$ distinct roots.

8.1.3 Fall 2019 Midterm #10 ✨

Let L/K be a finite normal extension.

a. Show that if L/K is cyclic and E/K is normal with $L/E/K$ then L/E and E/K are cyclic.

b. Show that if L/K is cyclic then there exists exactly one extension E/K of degree n with $L/E/K$ for each divisor n of $[L : K]$.

Solution:
The setup:

$$\begin{tikzcd}
L \\
E \arrow[u, "g"'] \\
K \arrow[u, "n"'] \arrow[uu, bend left=40, "g"]
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
1 \arrow[d] \arrow[dd, bend left=40] \\
H \coloneqq \mathsf{Gal}(L/E) \arrow[d, "n"] \\
G \coloneqq \mathsf{Gal}(L/K) = C_n
\end{tikzcd}$$

Link to Diagram

Part 1:

- L/K is cyclic means L/K is Galois and $G \coloneqq \mathsf{Gal}(L/K) = C_n$ for some n.
- By the FTGT, setting $H \coloneqq \mathsf{Gal}(L/E)$, we get $H \trianglelefteq G$ precisely because E/K is normal, and $\mathsf{Gal}(L/E) = G/H$.
- But then if G is cyclic, $H \leq G$ must be cyclic, and G/H is cyclic as well since writing $G = C_n = \langle x \rangle$, we have $G/H = \langle xH \rangle$.

Part 2:

- Letting $G \coloneqq \mathsf{Gal}(L/K) = C_n$, by elementary group theory we have subgroups $H \coloneqq C_d \leq C_n$ for every d dividing n.
  - A observation we'll need: every subgroup is normal here since G is abelian.
- By the fundamental theorem, taking the fixed field of $H \leq \mathsf{Gal}(L/K)$, we obtain some intermediate extension $E \coloneqq K^H$ fitting into a tower $L/E/K$.
- By the fundamental theorem, $[E : K] = [G : H] = n/d$, where we've used that $H \trianglelefteq G$.
- Letting d range through divisors lets n/d range through divisors, so we get extensions of every degree d dividing n.

8.1.4 Fall 2019 Midterm #8 🚩

Let k be a field of characteristic $p \neq 0$ and $f \in k[x]$ irreducible. Show that $f(x) = g(x^{p^d})$ where $g(x) \in k[x]$ is irreducible and separable.

Conclude that every root of f has the same multiplicity p^d in the splitting field of f over k.

8.1.5 Fall 2019 Midterm #7 🚩

Show that a field k of characteristic $p \neq 0$ is perfect $\iff$ for every $x \in k$ there exists a $y \in k$ such that $y^p = x$.

8.1.6 Spring 2012 #4 🚩

Let $f(x) = x^7 - 3 \in \mathbb{Q}[x]$ and $E/\mathbb{Q}$ be a splitting field of f with $\alpha \in E$ a root of f.

a. Show that E contains a primitive 7th root of unity.

b. Show that $E \neq \mathbb{Q}(\alpha)$.

8.1.7 Fall 2013 #5 ✨

Let L/K be a finite extension of fields.

a. Define what it means for L/K to be *separable.*

b. Show that if K is a finite field, then L/K is always separable.

c. Give an example of a finite extension L/K that is not separable.

Solution:

- L/k is **separable** iff every element α is separable, i.e. the minimal polynomial $m(x)$ of α is a separable polynomial, i.e. $m(x)$ has no repeated roots in (say) the algebraic closure of L (or just any splitting field of m).
- If $\operatorname{ch} k = p$, suppose toward a contradiction that L/k is not separable. Then there is some α with an inseparable (and irreducible) minimal polynomial $f(x) \in k[x]$.
- Claim: since f is inseparable and irreducible, $f(x) = g(x^p)$ for some $g \in k[x]$.
  - Note: write $g(x) := \sum a_k x^k$, so that $f(x) = \sum a_k (x^p)^k = \sum a_k x^{pk}$.

- This is a contradiction, since it makes f reducible by using the "Freshman's dream":

$$f(x) = \sum a_k x^{pk} = \left(\sum a_k^{\frac{1}{p}} x^k \right)^p := (h(x))^p.$$

- Proof of claim: in $\operatorname{ch} k = p, f$ inseparable $\implies f(x) = g(x^p)$.
  - Use that f is inseparable iff $\gcd(f, f') \neq 1$, and since f is irreducible this forces $f' \equiv 0$, so $ka_k = 0$ for all k.
  - Then $a_k \neq 0$ forces $p \mid k$, so $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots$ and one takes $g(x) := \sum a_{kp} x^{kp}$.
- A finite inseparable extension:
  - It's a theorem that finite extensions of perfect fields are separable, so one needs a non-perfect field.
  - Take $L/k := \mathbb{F}_p(t^{\frac{1}{p}})/\mathbb{F}_p(t)$, which is a degree p extension (although both fields are infinite are characteristic p).
  - Then the minimal polynomial of t is $f(x) := x^p - t \in \mathbb{F}_p(t)[x]$, where $f'(x) = px^p \equiv 0$ Alternatively, just note that f factors as $f(x) = (x - t^{\frac{1}{p}})^p$ in $L[x]$, which has multiple roots.

8.1.8 Fall 2012 #4

Let $f(x) \in \mathbb{Q}[x]$ be a polynomial and K be a splitting field of f over $\mathbb{Q}$. Assume that $[K : \mathbb{Q}] = 1225$ and show that $f(x)$ is solvable by radicals.

8.2 Galois Groups: Concrete Computations

8.2.1 Exercise: $G(x^2 - 2)$

Exercise 8.2.1 (?)
Compute the Galois group of $x^2 - 2$.

Solution:
$\mathbb{Z}/2\mathbb{Z}$?

8.2.2 Exercise: $G(x^p - 2)$

Exercise 8.2.2 (?)
Let $p \in \mathbb{Z}$ be a prime number. Then describe the elements of the Galois group of the polynomial $x^p - 2$.

Solution:
$\mathbb{Q}(2^{\frac{1}{p}}, \zeta_p)$, which has degree $p(p-1)$ and is generated by the maps

$$\sqrt[p]{2} \mapsto \sqrt[p]{2}\zeta^a$$
$$\zeta \mapsto \zeta^b.$$

8.2.3 Fall 2020 #3

a. Define what it means for a finite extension of fields E over F to be a *Galois* extension.

b. Determine the Galois group of $f(x) = x^3 - 7$ over $\mathbb{Q}$, and justify your answer carefully.

c. Find all subfields of the splitting field of $f(x)$ over $\mathbb{Q}$.

Solution:
Part a:

- A finite extension E/F is **Galois** if it is normal and separable:
  - Normal: every $f \in F[x]$ either has no roots in E or all roots in E.
  - Separable: every element $e \in E$ has a separable minimal polynomial $m(x)$, i.e. m has no repeated roots.

Part b:

- Note f is irreducible by Eisenstein with $p = 7$, and since $\mathbb{Q}$ is perfect, irreducible implies separable.

- Writing $L := \mathrm{SF}(f)/\mathbb{Q}$, this is a Galois extension:
  - L is separable: it is a finite extension of a perfect field, which is automatically separable.
  - L is normal: L is the splitting field of a separable polynomial, and thus normal.

- Since f is degree 3, we have $G := \mathsf{Gal}(L/k) \leq S_3$, and since G is a transitive subgroup the only possibilities are

$$G = S_3 \cong D_3, A_3 \cong C_3.$$

- Factor $x^3 - 7 = (x - \omega)(x - \zeta_3\omega)(x - \zeta_3^2\omega)$ where $\omega := 7^{\frac{1}{3}}$ and ζ_3 is a primitive 3rd root of unity. Then $L = \mathbb{Q}(\zeta_3, \omega)$.

  - Aside: label the roots in this order, so $r_1 = \omega, r_2 = \zeta_3\omega, r_3 = \zeta_3^2\omega$.

- Write $\min_{\omega,\mathbb{Q}}(x) = x^3 - 7$ and let $L_0/\mathbb{Q} := \mathbb{Q}(\omega)/\mathbb{Q}$ yields $[L_0 : \mathbb{Q}] = 3$.
- Write $\min_{\zeta_3,\mathbb{Q}}(x) = (x^3-1)/(x-1) = x^2+x+1$, and note that this is still the minimal polynomial over L_0 since $L_0 \subseteq \mathbb{R}$ and $\zeta_3 \in \mathbb{C} \setminus \mathbb{R}$. So $[L : L_0] = 2$.
- Counting in towers,

$$[L : \mathbb{Q}] = [L : L_0][L_0 : \mathbb{Q}] = (2)(3) = 6.$$

- But $\#S_3 = 6$ and $\#A_3 = 3$, so $G = S_3$.
- Explicitly, since we can write $\mathrm{SF}(f) = \mathbb{Q}(\omega, \zeta_3)$, we can find explicit generators:

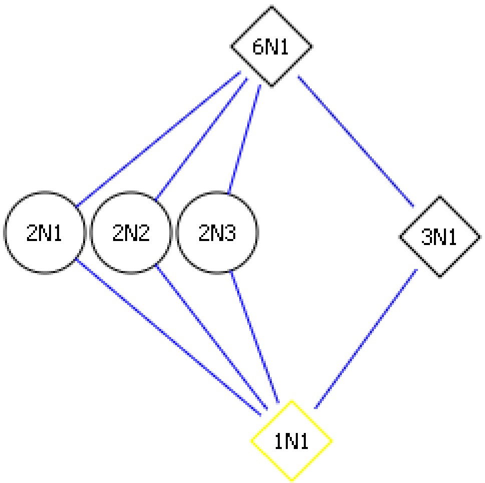
$$\sigma : \begin{cases} \omega & \mapsto \omega \\ \zeta_3 & \mapsto \zeta_3 \cdot \zeta_3. \end{cases} \qquad \implies \sigma \sim (1,2,3)$$

$$\tau : \begin{cases} \omega & \mapsto \omega \\ \zeta_3 & \mapsto \overline{\zeta_3}. \end{cases} \qquad \implies \tau \sim (2,3).$$

So $G = \left\langle \sigma, \tau \mid \sigma^3, \tau^2 \right\rangle$.

Part c:

- Note that the subgroup lattice for S_3 looks like the following:



- Note that we can identify
  - $\tau = (2,3)$ which fixes r_1
  - $\sigma\tau = (1,2)$ which fixes r_3
  - $\sigma^2\tau = (1,3)$ which fixes r_2

- $\sigma = (1,2,3)$, for which we need to calculate the fixed field. Using that $\sigma(\omega) = \zeta\omega$ and $\sigma(\zeta) = \zeta$, supposing $\sigma(\alpha) = \alpha$ we have

$$\begin{aligned}
\sigma(\alpha) &\coloneqq \sigma(a + b\zeta_3 + c\zeta_3^2 + d\omega + e\zeta_3\omega + f\zeta_3^2\omega) \\
&= a + b\zeta_3 + c\zeta_3^2 + d\zeta_3\omega + e\zeta_3^2\omega + f\omega \\
\implies \alpha &= a + b\zeta_3 + c\zeta_3^2 + t_1(\omega + \zeta_3\omega + \zeta_3^2\omega) \\
\implies \alpha &= a + b\zeta_3 + c\zeta_3^2 + t_1\omega(1 + \zeta_3 + \zeta_3^2) \\
\implies \alpha &= a + b\zeta_3 + c\zeta_3^2,
\end{aligned}$$

using the general fact that $\sum_{k=0}^{n-1} \zeta_n^k = 0$. So the fixed field is $\mathbb{Q}(1, \zeta, \zeta^2) = \mathbb{Q}(\zeta)$.

- We thus get the following lattice correspondence:

$$\begin{tikzcd}
 & & \mathbb{Q}(\zeta_3, \omega) & \\
\mathbb{Q}(\omega) = \mathbb{Q}(r_1) \arrow[urr, "2"] & \mathbb{Q}(\zeta_3\omega) = \mathbb{Q}(r_2) \arrow[ur, "2"] & \mathbb{Q}(\zeta_3^2\omega) = \mathbb{Q}(r_3) \arrow[u, "2"] & \mathbb{Q}(\zeta_3) \arrow[ul, "3"] \\
 & & \mathbb{Q} \arrow[ull, "3"] \arrow[ul, "3"] \arrow[u, "3"] \arrow[ur, "2"] &
\end{tikzcd}$$

$$\begin{tikzcd}
 & & 1 \arrow[dll, "2"] \arrow[dl, "2"] \arrow[d, "2"] \arrow[dr, "3"] & \\
\langle (2,3) = \tau \rangle \cong C_2 \arrow[drr, "3"] & \left\langle (1,3) = \sigma^2\tau \right\rangle \cong C_2 \arrow[dr, "3"] & \langle (1,2) = \sigma\tau \rangle \cong C_2 \arrow[d, "3"] & \langle (1,2,3) = \sigma \rangle \cong C_3 \arrow[dl, "2"] \\
 & & \langle \sigma, \tau \rangle \cong S_3 &
\end{tikzcd}$$

Link to Diagram

8.2.4 Spring 2021 #4 🚩

Define

$$f(x) \coloneqq x^4 + 4x^2 + 64 \in \mathbb{Q}[x].$$

a. Find the splitting field K of f over $\mathbb{Q}$.

b. Find the Galois group G of f.

c. Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and K.

Concepts Used:

- Useful trick: given $a+\sqrt{b}$, try to rewrite this as $(\sqrt{c}+\sqrt{d})^2$ for some c, d to get a better basis for $\mathrm{SF}(f)$.

Solution:

- First consider $g(z) \coloneqq z^2+4z+64$. Applying the quadratic formula yields

$$z = \frac{-4 \pm \sqrt{16-64}}{2} = -2 \pm \frac{1}{2}\sqrt{-15 \cdot 16} = -2 \pm 2i\sqrt{15}.$$

- Substituting $z = x^2$ yields the splitting field of f as $L \coloneqq \mathbb{Q}(\pm\sqrt{-2 \pm 2i\sqrt{15}})$.
  - Note that this factorization shows that f is irreducible over $\mathbb{Q}$, since the two quadratic factors have irrational coefficients and none of the roots are real.
  - Irreducible implies separable over a perfect field, so $L/\mathbb{Q}$ is a separable extension.
  - L is the splitting field of a separable polynomial and thus normal, making L Galois.

- In this form, it's not clear what the degree $[L : \mathbb{Q}]$ is, so we can find a better basis by rewriting the roots of g:

$$z = -2 \pm 2i\sqrt{15} = \left(\sqrt{5}\right)^2 - \left(\sqrt{3}\right)^2 \pm 2i\sqrt{5}\sqrt{3} = (\sqrt{5} \pm i\sqrt{3})^2,$$

  and so the roots of f are $x = \pm\sqrt{5} \pm i\sqrt{3}$ and $L = \mathbb{Q}(\sqrt{5}, i\sqrt{3})$.

- Counting in towers,

$$[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, i\sqrt{3}) : \mathbb{Q}\sqrt{5}][\mathbb{Q}\sqrt{5} : \mathbb{Q}] = (2)(2) = 4,$$

  where we've used that $\min_{\sqrt{5},\mathbb{Q}}(x) = x^2-5$ and $\min_{i\sqrt{3},\mathbb{Q}}(x) = x^2+3$, which remains the minimal polynomial over $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{R}$ since both roots are not real.

- So $G \coloneqq \mathsf{Gal}(L/\mathbb{Q}) \leq S_4$ is a transitive subgroup of size 4, making it either C_4 or C_2^2.

- Label the roots:

$$\begin{aligned} r_1 &= \sqrt{5}+i\sqrt{3} \\ r_2 &= \sqrt{5}-i\sqrt{3} \\ r_3 &= -\sqrt{5}+i\sqrt{3} = -r_2 \\ r_4 &= -\sqrt{5}-i\sqrt{3} = -r_1. \end{aligned}$$

- We can start writing down automorphisms:

$$\sigma_1 : \begin{cases} \sqrt{5} & \mapsto -\sqrt{5} \\ i\sqrt{3} & \mapsto i\sqrt{3}. \end{cases} \qquad \sigma_1 \sim (1,3)(2,4)$$

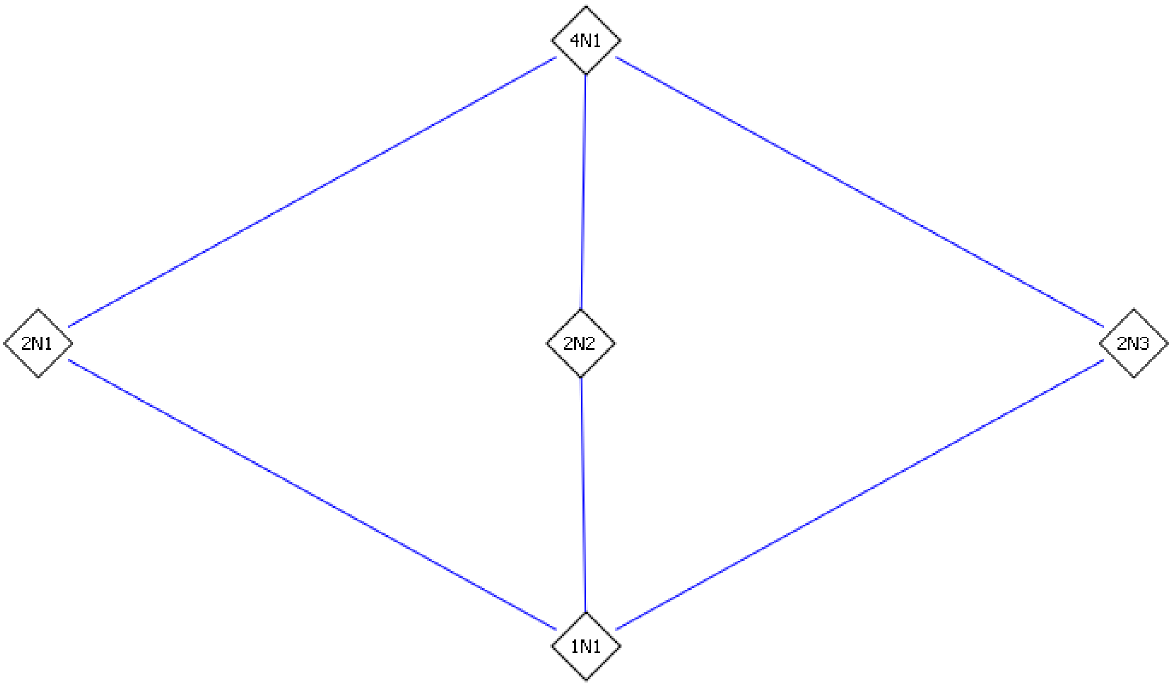
$$\sigma_2 \begin{cases} \sqrt{5} & \mapsto \sqrt{5} \\ i\sqrt{3} & \mapsto -i\sqrt{3}. \end{cases} \qquad \sigma_2 \sim (1,2)(3,4).$$

  Note that these define automorphisms because we've specified what happens to a basis and they send roots to other roots.

- Checking that $\sigma_1^2 = \sigma_2^2 = \mathrm{id}$, this produces two distinct order 2 elements, forcing $G \cong C_2^2$ since C_4 only has one order 2 element. Explicitly, we have

$$C_2^2 \cong G = \langle \tau_1, \tau_2 \rangle = \{\mathrm{id}, \tau_1, \tau_2, \tau_1\tau_2\} = \{\mathrm{id}, (1,3)(2,4), (1,2)(3,4), (1,4)(2,3)\},$$

  and the generic subgroup lattice looks like:



- Computing some fixed fields. Write $i\sqrt{3} = x, \sqrt{5} = y$, then elements in the splitting field are of the form $\alpha = 1 + ax + by + cxy$.

  - For σ_1, we have $x \mapsto -x$, so

$$\sigma_1(\alpha) = 1 - ax + by - cxy = \alpha \implies a = -a = 0, c = -c = 0,$$

    so this preserves $1 + by$, making the fixed field $\mathbb{Q}(1, y) = \mathbb{Q}(i\sqrt{3})$.

- For σ_2, we have $y \mapsto -y$, so

$$\sigma_2(\alpha) = 1 + ax - by - cxy = \alpha \implies b = -b = 0, c = -c = 0,$$

preserving $1 + ax$ and making the fixed field $\mathbb{Q}(1, x) = \mathbb{Q}(\sqrt{5})$.

- For $\sigma_1\sigma_2$, we have $x \mapsto -x$ and $y \mapsto -y$, so

$$\sigma_1\sigma_2(\alpha) = 1 - ax - by + cxy = \alpha \implies a = -a = -, b = -b = 0,$$

preserving $1 + cxy$ and yielding $\mathbb{Q}(xy) = \mathbb{Q}(i\sqrt{3}\sqrt{5})$.

- So the lattice correspondence we get here is

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{5}, i\sqrt{3}) & \\
\mathbb{Q}(i\sqrt{3}) \arrow[ur, "2" description] & \mathbb{Q}(i\sqrt{3}\sqrt{5}) \arrow[u, "2" description] & \mathbb{Q}(\sqrt{5}) \arrow[ul, "2" description] \\
& \mathbb{Q} \arrow[ul, "2" description] \arrow[u, "2" description] \arrow[ur, "2" description] &
\end{tikzcd}$$

$$\begin{tikzcd}
& 1 \arrow[dl, "2" description] \arrow[d, "2" description] \arrow[dr, "2" description] & \\
\langle \sigma_1 \rangle \arrow[dr, "2" description] & \langle \sigma_1\sigma_2 \rangle \arrow[d, "2" description] & \langle \sigma_2 \rangle \arrow[dl, "2" description] \\
& G = \langle \tau_1, \tau_2 \rangle &
\end{tikzcd}$$

Link to Diagram

8.2.5 Fall 2019 Midterm #6

Compute the Galois group of $f(x) = x^3 - 3x - 3 \in \mathbb{Q}[x]/\mathbb{Q}$.

8.2.6 Spring 2018 #2 ✨

Let $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$.

a. Find the splitting field K of f, and compute $[K : \mathbb{Q}]$.

b. Find the Galois group G of f, both as an explicit group of automorphisms, and as a familiar abstract group to which it is isomorphic.

c. Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and k.

Not the nicest proof! Would be better to replace the ad-hoc computations at the end.

Solution:

Proof (of a).
Note that $g(x) = x^2 - 4x + 2$ has roots $\beta = 2 \pm \sqrt{2}$, and so f has roots

$$\begin{aligned}
\alpha_1 &= \sqrt{2 + \sqrt{2}} \\
\alpha_2 &= \sqrt{2 - \sqrt{2}} \\
\alpha_3 &= -\alpha_1 \\
\alpha_4 &= -\alpha_2.
\end{aligned}$$

and splitting field $K = \mathbb{Q}(\{\alpha_i\})$.

■

Proof (of b).
K is the splitting field of a separable polynomial and thus Galois over $\mathbb{Q}$. Moreover, Since f is irreducible by Eisenstein with $p = 2$, the Galois group is a transitive subgroup of S^4, so the possibilities are:

- S_4
- A_4
- D_4
- $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$
- $\mathbb{Z}/(4)$

We can note that g splits over $L := \mathbb{Q}(\sqrt{2})$, an extension of degree 2.
We can now note that $\min(\alpha, L)$ is given by $p(x) = x^2 - (2 + \sqrt{2})$, and so $[K : L] = 2$. We then have

$$[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] = (2)(2) = 4.$$

This $|\mathsf{Gal}(K/\mathbb{Q})| = 4$, which leaves only two possibilities:

- $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$
- $\mathbb{Z}/(4)$

We can next check orders of elements. Take

$$\begin{aligned} \sigma &\in \mathsf{Gal}(K/\mathbb{Q}) \\ \alpha_1 &\mapsto \alpha_2. \end{aligned}$$

Computations show that

- $\alpha_1^2 \alpha_2^2 = 2$, so $\alpha_1 \alpha_2 = \sqrt{2}$
- $\alpha_1^2 = 2 + \sqrt{2} \implies \sqrt{2} = \alpha_1^2 - 2$

and thus

$$\begin{aligned} \sigma^2(\alpha_1) &= \sigma(\alpha_2) \\ &= \sigma\left(\frac{\sqrt{2}}{\alpha_1}\right) \\ &= \frac{\sigma(\sqrt{2})}{\sigma(\alpha_1)} \\ &= \frac{\sigma(\alpha_1^2 - 2)}{\alpha_2} \\ &= \frac{\alpha_2^2 - 2}{\alpha_2} \\ &= \alpha_2 - 2\alpha_2^{-1} \\ &= \alpha_2 - \frac{2\alpha_1}{\sqrt{2}} \\ &= \alpha_2 - \alpha_1\sqrt{2} \\ &\neq \alpha_1, \end{aligned}$$

and so the order of σ is strictly greater than 2, and thus 4, and thus $\mathsf{Gal}(K/\mathbb{Q}) = \left\{\sigma^k \;\middle|\; 1 \leq k \leq 4\right\} \cong \mathbb{Z}/(4)$.

■

Proof (of c).

?? The subgroup of index 2 $\left\langle \sigma^2 \right\rangle$ corresponds to the field extension $Q(\sqrt{2})/\mathbb{Q}$. ■

Finish (c)

8.2.7 Spring 2020 #4 🚩

Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.

a. Define what it means for a finite extension field E of a field F to be a Galois extension.

b. Determine the Galois group $\operatorname{Gal}(E/\mathbb{Q})$ for the polynomial $f(x)$, and justify your answer carefully.

c. Exhibit a subfield K in (b) such that $\mathbb{Q} \leq K \leq E$ with K not a Galois extension over $\mathbb{Q}$. Explain.

8.2.8 Spring 2017 #8 🚩

a. Let K denote the splitting field of $x^5 - 2$ over $\mathbb{Q}$. Show that the Galois group of $K/\mathbb{Q}$ is isomorphic to the group of invertible matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \quad \text{where} \quad a \in \mathbb{F}_5^\times \text{ and } b \in \mathbb{F}_5.$$

b. Determine all intermediate fields between K and $\mathbb{Q}$ which are Galois over $\mathbb{Q}$.

8.2.9 Fall 2016 #4 🚩

Set $f(x) = x^3 - 5 \in \mathbb{Q}[x]$.

a. Find the splitting field K of $f(x)$ over $\mathbb{Q}$.

b. Find the Galois group G of K over $\mathbb{Q}$.

c. Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and K.

8.2.10 Spring 2016 #2

Let $K = \mathbb{Q}[\sqrt{2} + \sqrt{5}]$.

a. Find $[K : \mathbb{Q}]$.

b. Show that $K/\mathbb{Q}$ is Galois, and find the Galois group G of $K/\mathbb{Q}$.

c. Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and K.

8.2.11 Fall 2015 #5

Let $u = \sqrt{2+\sqrt{2}}$, $v = \sqrt{2-\sqrt{2}}$, and $E = \mathbb{Q}(u)$.

a. Find (with justification) the minimal polynomial $f(x)$ of u over $\mathbb{Q}$.

b. Show $v \in E$, and show that E is a splitting field of $f(x)$ over $\mathbb{Q}$.

c. Determine the Galois group of E over $\mathbb{Q}$ and determine all of the intermediate fields F such that $\mathbb{Q} \subset F \subset E$.

8.2.12 Spring 2015 #5

Let $f(x) = x^4 - 5 \in \mathbb{Q}[x]$.

a. Compute the Galois group of f over $\mathbb{Q}$.

b. Compute the Galois group of f over $\mathbb{Q}(\sqrt{5})$.

8.2.13 Fall 2014 #3

Consider the polynomial $f(x) = x^4 - 7 \in \mathbb{Q}[x]$ and let $E/\mathbb{Q}$ be the splitting field of f.

a. What is the structure of the Galois group of $E/\mathbb{Q}$?

b. Give an explicit description of all of the intermediate subfields $\mathbb{Q} \subset K \subset E$ in the form $K = \mathbb{Q}(\alpha), \mathbb{Q}(\alpha, \beta), \cdots$ where α, β, etc are complex numbers. Describe the corresponding subgroups of the Galois group.

8.2.14 Fall 2013 #6

Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$ and set $G = \mathrm{Gal}(K/\mathbb{Q})$.

a. Show that $K/\mathbb{Q}$ contains both $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt[4]{2})$ and has degree 8 over $\mathbb{Q}/$

b. Let $N = \mathrm{Gal}(K/\mathbb{Q}(i))$ and $H = \mathrm{Gal}(K/\mathbb{Q}(\sqrt[4]{2}))$. Show that N is normal in G and $NH = G$.

Hint: what field is fixed by NH?

c. Show that $\mathrm{Gal}(K/\mathbb{Q})$ is generated by elements σ, τ, of orders 4 and 2 respectively, with $\tau\sigma\tau^{-1} = \sigma^{-1}$.

Equivalently, show it is the dihedral group of order 8.

d. How many distinct quartic subfields of K are there? Justify your answer.

8.2.15 Spring 2014 #4

Let $E \subset \mathbb{C}$ denote the splitting field over $\mathbb{Q}$ of the polynomial $x^3 - 11$.

a. Prove that if n is a squarefree positive integer, then $\sqrt{n} \notin E$.

Hint: you can describe all quadratic extensions of $\mathbb{Q}$ contained in E.

b. Find the Galois group of $(x^3 - 11)(x^2 - 2)$ over $\mathbb{Q}$.

c. Prove that the minimal polynomial of $11^{1/3} + 2^{1/2}$ over $\mathbb{Q}$ has degree 6.

8.2.16 Spring 2013 #8

Let F be the field with 2 elements and K a splitting field of $f(x) = x^6 + x^3 + 1$ over F. You may assume that f is irreducible over F.

a. Show that if r is a root of f in K, then $r^9 = 1$ but $r^3 \neq 1$.

b. Find $\mathrm{Gal}(K/F)$ and express each intermediate field between F and K as $F(\beta)$ for an appropriate $\beta \in K$.

8.3 Galois Groups: Indirect Computations / Facts

8.3.1 Fall 2019 #7 ✨

Let ζ_n denote a primitive nth root of $1 \in \mathbb{Q}$. You may assume the roots of the minimal polynomial $p_n(x)$ of ζ_n are exactly the primitive nth roots of 1.

Show that the field extension $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is Galois and prove its Galois group is $(\mathbb{Z}/n\mathbb{Z})^\times$.

How many subfields are there of $\mathbb{Q}(\zeta_{20})$?

Concepts Used:

- **Galois** = normal + separable.
- **Separable**: Minimal polynomial of every element has distinct roots.
- **Normal (if separable)**: Splitting field of an irreducible polynomial.
- ζ is a primitive root of unity $\iff$ $o(\zeta) = n$ in $\mathbb{F}^\times$.
- $\varphi(p^k) = p^{k-1}(p-1)$
- The lattice:

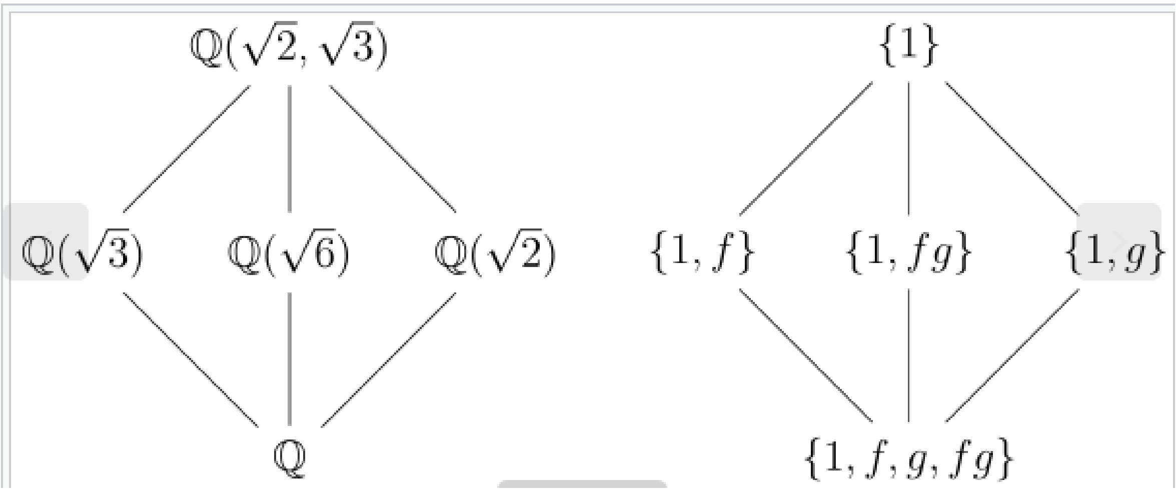


Figure 1: image_2021-04-17-02-44-48

Solution:
Let $K = \mathbb{Q}(\zeta)$. Then K is the splitting field of $f(x) = x^n - 1$, which is irreducible over $\mathbb{Q}$, so $K/\mathbb{Q}$ is normal. We also have $f'(x) = nx^{n-1}$ and $\gcd(f, f') = 1$ since they can not share any

roots.

Or equivalently, f splits into distinct linear factors $f(x) = \prod_{k \leq n} (x - \zeta^k)$.

Since it is a Galois extension, $|\mathsf{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = \varphi(n)$ for the totient function.
We can now define maps

$$\begin{aligned} \tau_j : K &\to K \\ \zeta &\mapsto \zeta^j \end{aligned}$$

and if we restrict to j such that $\gcd(n, j) = 1$, this yields $\varphi(n)$ maps. Noting that if ζ is a primitive root, then $(n, j) = 1$ implies that that ζ^j is also a primitive root, and hence another root of $\min(\zeta, \mathbb{Q})$, and so these are in fact automorphisms of K that fix $\mathbb{Q}$ and thus elements of $\mathsf{Gal}(K/\mathbb{Q})$.
So define a map

$$\begin{aligned} \theta : \mathbb{Z}_n^\times &\to K \\ [j]_n &\mapsto \tau_j. \end{aligned}$$

from the *multiplicative* group of units to the Galois group.
The claim is that this is a surjective homomorphism, and since both groups are the same size, an isomorphism.

Proof (of surjectivity).
Letting $\sigma \in K$ be arbitrary, noting that $[K : \mathbb{Q}]$ has a basis $\left\{1, \zeta, \zeta^2, \cdots, \zeta^{n-1}\right\}$, it suffices to specify $\sigma(\zeta)$ to fully determine the automorphism. (Since $\sigma(\zeta^k) = \sigma(\zeta)^k$.)
In particular, $\sigma(\zeta)$ satisfies the polynomial $x^n - 1$, since $\sigma(\zeta)^n = \sigma(\zeta^n) = \sigma(1) = 1$, which means $\sigma(\zeta)$ is another root of unity and $\sigma(\zeta) = \zeta^k$ for some $1 \leq k \leq n$.
Moreover, since $o(\zeta) = n \in K^\times$, we must have $o(\zeta^k) = n \in K^\times$ as well. Noting that $\left\{\zeta^i\right\}$ forms a cyclic subgroup $H \leq K^\times$, then $o(\zeta^k) = n \iff (n, k) = 1$ (by general theory of cyclic groups).
Thus θ is surjective.

■

Proof (of being a homomorphism).

$$\tau_j \circ \tau_k(\zeta) = \tau_j(\zeta^k) = \zeta^{jk} \implies \tau_{jk} = \theta(jk) = \tau_j \circ \tau_k.$$

■

Proof (of part 2).
We have $K \cong \mathbb{Z}_{20}^\times$ and $\varphi(20) = 8$, so $K \cong \mathbb{Z}_8$, so we have the following subgroups and corresponding intermediate fields:

- $0 \sim \mathbb{Q}(\zeta_{20})$
- $\mathbb{Z}_2 \sim \mathbb{Q}(\omega_1)$
- $\mathbb{Z}_4 \sim \mathbb{Q}(\omega_2)$
- $\mathbb{Z}_8 \sim \mathbb{Q}$

For some elements ω_i which exist by the primitive element theorem.

■

8.3.2 Fall 2018 #3 ✨

Let $F \subset K \subset L$ be finite degree field extensions. For each of the following assertions, give a proof or a counterexample.

a. If L/F is Galois, then so is K/F.

b. If L/F is Galois, then so is L/K.

c. If K/F and L/K are both Galois, then so is L/F.

Concepts Used:

- Every quadratic extension over $\mathbb{Q}$ is Galois.

Solution:
Let $L/K/F$.

Proof (of a).
False: Take $L/K/F = \mathbb{Q}(\zeta_2, \sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}$.
Then L/F is Galois, since it is the splitting field of $x^3 - 2$ and $\mathbb{Q}$ has characteristic zero.
But K/F is not Galois, since it is not the splitting field of any irreducible polynomial.

■

Proof (of b).
True: If L/F is Galois, then L/K is normal and separable:

- L/K is normal, since if $\sigma : L \hookrightarrow \overline{K}$ lifts the identity on K and fixes L, i-t also lifts the identity on F and fixes L (and $\overline{K} = \overline{F}$).
- L/K is separable, since $F[x] \subseteq K[x]$, and so if $\alpha \in L$ where $f(x) := \min(\alpha, F)$ has no repeated factors, then $f'(x) := \min(\alpha, K)$ divides f and thus can not have repeated factors.

■

Proof (of c).
False: Use the fact that every quadratic extension is Galois, and take $L/K/F = \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}$.
Then each successive extension is quadratic (thus Galois) but $\mathbb{Q}(\sqrt[4]{2})$ is not the splitting field of any polynomial (noting that it does not split $x^4 - 2$ completely.)

■

8.3.3 Spring 2018 #3 ✨

Let K be a Galois extension of $\mathbb{Q}$ with Galois group G, and let E_1, E_2 be intermediate fields of K which are the splitting fields of irreducible $f_i(x) \in \mathbb{Q}[x]$.

Let $E = E_1 E_2 \subset K$.

Let $H_i = \mathsf{Gal}(K/E_i)$ and $H = \mathsf{Gal}(K/E)$.

a. Show that $H = H_1 \cap H_2$.

b. Show that $H_1 H_2$ is a subgroup of G.

c. Show that

$$\mathsf{Gal}(K/(E_1 \cap E_2)) = H_1 H_2.$$

Concepts Used:

- The Galois correspondence:
  - $H_1 \cap H_2 \rightleftharpoons E_1 E_2$,
  - $H_1 H_2 \rightleftharpoons E_1 \cap E_2$.

Solution:

Proof (of a).
By the Galois correspondence, it suffices to show that the fixed field of $H_1 \cap H_2$ is E_1E_2. Let $\sigma \in H_1 \cap H_2$; then $\sigma \in \operatorname{Aut}(K)$ fixes both E_1 and E_2.

Not sure if this works – compositum is not literally product..?

Writing $x \in E_1E_2$ as $x = e_1e_2$, we have

$$\sigma(x) = \sigma(e_1e_2) = \sigma(e_1)\sigma(e_2) = e_1e_2 = x,$$

so σ fixes E_1E_2.

■

Proof (of b).
That $H_1H_2 \subseteq G$ is clear, since if $\sigma = \tau_1\tau_2 \in H_1H_2$, then each τ_i is an automorphism of K that fixes $E_i \supseteq \mathbb{Q}$, so each τ_i fixes $\mathbb{Q}$ and thus σ fixes $\mathbb{Q}$.

Claim: All elements in this subset commute.

Proof (of claim).

- Let $\sigma = \sigma_1\sigma_2 \in H_1H_2$.
- Note that $\sigma_1(e) = e$ for all $e \in E_1$ by definition, since H_1 fixes E_1, and $\sigma_2(e) \in E_1$ (?).
- Then

  $$\sigma_1(e) = e \quad \forall e \in E_1 \implies \sigma_1(\sigma_2(e)) = \sigma_2(e)$$

  and substituting $e = \sigma_1(e)$ on the RHS yields

  $$\sigma_1\sigma_2(e) = \sigma_2\sigma_1(e),$$

  where a similar proof holds for $e \in E_2$ and thus for arbitrary $x \in E_1E_2$.

■

■

Proof (of c).
By the Galois correspondence, the subgroup $H_1 H_2 \leq G$ will correspond to an intermediate field E such that $K/E/\mathbb{Q}$ and E is the fixed field of $H_1 H_2$.
But if $\sigma \in H_1 H_2$, then $\sigma = \tau_1 \tau_2$ where τ_i is an automorphism of K that fixes E_i, and so

$$\begin{aligned} \sigma(x) = x \iff \tau_1\tau_2(x) = x &\iff \tau_2(x) = x \\ &\& \\ \tau_1(x) = x &\iff x \in E_1 \cap E_2. \end{aligned}$$

.

■

8.3.4 Fall 2017 #4

a. Let $f(x)$ be an irreducible polynomial of degree 4 in $\mathbb{Q}[x]$ whose splitting field K over $\mathbb{Q}$ has Galois group $G = S_4$.

   Let θ be a root of $f(x)$. Prove that $\mathbb{Q}[\theta]$ is an extension of $\mathbb{Q}$ of degree 4 and that there are no intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}[\theta]$.

b. Prove that if K is a Galois extension of $\mathbb{Q}$ of degree 4, then there is an intermediate subfield between K and $\mathbb{Q}$.

8.3.5 Spring 2017 #7

Let F be a field and let $f(x) \in F[x]$.

a. Define what a splitting field of $f(x)$ over F is.

b. Let F now 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 $g(x)$ over F. Fully justify your answer.

c. Show that the extension E/F in (b) is a Galois extension.

8.3.6 Spring 2016 #6

Let K be a Galois extension of a field F with $[K : F] = 2015$. Prove that K is an extension by radicals of the field F.

8.3.7 Fall 2015 #6

a. Let G be a finite group. Show that there exists a field extension K/F with $\mathrm{Gal}(K/F) = G$.

You may assume that for any natural number n there is a field extension with Galois group S_n.

b. Let K be a Galois extension of F with $|\mathrm{Gal}(K/F)| = 12$. Prove that there exists an intermediate field E of K/F with $[E : F] = 3$.

c. With K/F as in (b), does an intermediate field L necessarily exist satisfying $[L : F] = 2$? Give a proof or counterexample.

8.3.8 Fall 2014 #1

Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial and L a finite Galois extension of $\mathbb{Q}$. Let $f(x) = g_1(x)g_2(x)\cdots g_r(x)$ be a factorization of f into irreducibles in $L[x]$.

a. Prove that each of the factors $g_i(x)$ has the same degree.

b. Give an example showing that if L is not Galois over $\mathbb{Q}$, the conclusion of part (a) need not hold.

8.3.9 Spring 2013 #7

Let $f(x) = g(x)h(x) \in \mathbb{Q}[x]$ and $E, B, C/\mathbb{Q}$ be the splitting fields of f, g, h respectively.

a. Prove that $\mathrm{Gal}(E/B)$ and $\mathrm{Gal}(E/C)$ are normal subgroups of $\mathrm{Gal}(E/\mathbb{Q})$.

b. Prove that $\mathrm{Gal}(E/B) \cap \mathrm{Gal}(E/C) = \{1\}$.

c. If $B \cap C = \mathbb{Q}$, show that $\mathrm{Gal}(E/B)\mathrm{Gal}(E/C) = \mathrm{Gal}(E/\mathbb{Q})$.

d. Under the hypothesis of (c), show that $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(E/B) \times \mathrm{Gal}(E/C)$.

e. Use (d) to describe $\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$ where $\alpha = \sqrt{2} + \sqrt{3}$.

8.3.10 Fall 2012 #3

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 5. Assume that f has all but two roots in $\mathbb{R}$. Compute the Galois group of $f(x)$ over $\mathbb{Q}$ and justify your answer.

8.4 pth Roots and $x^{p^k} - x$

8.4.1 Spring 2021 #7 ✨

Let p be a prime number and let F be a field of characteristic p. Show that if $a \in F$ is not a pth power in F, then $x^p - a \in F[x]$ is irreducible.

Strategy:

- Contradiction: go to splitting field, apply Freshman's dream.
- Use that this polynomial is ramified, and its only factors are $(x-a)$.

Solution (Likely the 'right' solution):

- Suppose a is not a pth power in F, then $f(x) \coloneqq x^p - a$ has no roots in F.
- Toward a contradiction, suppose f is reducible in $F[x]$.
- In $\operatorname{SF}(f)$, since $\operatorname{ch} F = p$ we have $f(x) = (x-\zeta)^p$ for some $\zeta = a^{\frac{1}{p}}$.
  - So if f is reducible in $F[x]$, we have $f(x) = p_1(x)p_2(x)$ where $p(x) = (x-\zeta)^q \in F[x]$ for some $1 \leq q < p$, since these are the only factors of f.
  - The claim is that $\zeta \in F$ as well, which is a contradiction since ζ is a pth root of a.
- We have $x^q - \zeta^q \in F[x]$, so $\zeta^q \in F$.
- We know $a = \zeta^p \in F$, and thus $\zeta^d = \zeta \in F$ for $d \coloneqq \gcd(p,n) = 1$. ↯
  - Why this is true: write $d = \gcd(p,n)$ in $\mathbb{Z}$ to obtain $d = tp + sn$ for some t, s.
  - Then $\zeta^d = \zeta^{tp+sn} = (\zeta^p)^t \cdot (\zeta^n)^s \in F$.

Strategy (for an alternative solution):

- By contrapositive, show that $f(x) \coloneqq x^p - a \in \mathbb{F}[x]$ reducible $\implies$ a is a pth power in $\mathbb{F}$.
- Eventually show $a^\ell = b^p$ for some $\ell \in \mathbb{N}$ and some $b \in \mathbb{F}$, then $\gcd(\ell, p) = 1$ forces $b = a$ and $\ell = p$.
- Use the fact that the constant term of any $g \in \mathbb{F}[x]$ is actually in $\mathbb{F}$.

Concepts Used:

- Reducible: $f \in \mathbb{F}[x]$ is reducible iff there exists $g, h \in \mathbb{F}[x]$ nonconstant with $f = gh$.
  - Importantly, this factorization needs to happen in $\mathbb{F}[x]$, since we can *always* find such factorizations in the splitting field $\operatorname{SF}(f)[x]$.
- Bezout's identity: $\gcd(p,q) = d \implies$ there exist $s, t \in \mathbb{Z}$ such that

$$sp + tq = d.$$

Solution:

- WTS: $f(x) := x^p - a \in \mathbb{F}[x]$ reducible $\implies$ f has a root in the *base field* $\mathbb{F}$.
- Write $f(x) = g(x)h(x)$ and factor $f(x) = \prod_{i=1}^{p}(x - r_i) \in \mathrm{SF}(f)[x]$ where the r_i are not necessarily distinct roots.
- WLOG, $g(x) = \prod_{i=1}^{\ell}(x - r_i)$ for some $1 \leq \ell \leq p-1$, i.e. rearrange the factors so that g is the first ℓ of them.
  - $\ell \neq 1, p$ since f is reducible, making g, h nonconstant.
- Set $R_\ell := \prod_{i=1}^{\ell} r_i$, which is the constant term in g, so $R_\ell \in \mathbb{F}$ since $g \in \mathbb{F}[x]$.
- Each r_i is a root of f, so $r_i^p - a = 0$ for all i, so $r_i^p = a$.
- Trick: what is the pth power of R_ℓ?

$$\begin{aligned}
R_\ell^p &:= \left(\prod_{i=1}^{\ell}\right)^p \\
&= \prod_{i=1}^{\ell} r_i^p \\
&= \prod_{i=1}^{\ell} a \\
&= a^\ell,
\end{aligned}$$

  so $R_\ell^p = a^\ell$.
- Use Bezout: $\gcd(\ell, p) = 1$ since p is prime, so write $tp + s\ell = 1$ for some $t, s \in \mathbb{Z}$
- Use this to build a root of f that's in $\mathbb{F}$: write

$$\begin{aligned}
a &= a^1 \\
&= a^{tp+s\ell} \\
&= a^{tp}a^{s\ell} \\
&= a^{tp}(a^\ell)^s \\
&= a^{tp}(R_\ell^p)^s \\
&= (a^t R_\ell^s)^p \\
&:= \beta^p,
\end{aligned}$$

  so $a = \beta^p$.
  - Check $\beta \in \mathbb{F}$: use that $R_\ell \in \mathbb{F}$ since it was a constant term of a polynomial in $\mathbb{F}[x]$, $a \in \mathbb{F}$ by assumption, and fields are closed under taking powers and products.

8.4.2 Fall 2019 #4 ✨

Let F be a finite field with q elements. Let n be a positive integer relatively prime to q and let ω be a primitive nth root of unity in an extension field of F. Let $E = F[\omega]$ and let $k = [E : F]$.

a. Prove that n divides $q^k - 1$.

b. Let m be the order of q in $\mathbb{Z}/n\mathbb{Z}^\times$. Prove that m divides k.

c. Prove that $m = k$.

Revisit, tricky!

Concepts Used:

- $\mathbb{F}^\times$ is always cyclic for $\mathbb{F}$ a field.
- Lagrange: $H \leq G \implies \#H \mid \#G$.

Solution:

Proof (of a).

- Since $|F| = q$ and $[E : F] = k$, we have $|E| = q^k$ and $|E^\times| = q^k - 1$.
- Noting that $\zeta \in E^\times$ we must have $n = o(\zeta) \mid |E^\times| = q^k - 1$ by Lagrange's theorem.

■

Proof (of b).

- Rephrasing (a), we have

$$\begin{aligned} n \mid q^k - 1 &\iff q^k - 1 \cong 0 \bmod n \\ &\iff q^k \cong 1 \bmod n \\ &\iff m := o(q) \mid k. \end{aligned}$$

■

Proof (of c).

- Since $m \mid k \iff k = \ell m$, (**claim**) there is an intermediate subfield M such that

$$E \leq M \leq F \quad k = [F : E] = [F : M][M : E] = \ell m,$$

  so M is a degree m extension of E.

- Now consider $M^{\times}$.
- By the argument in (a), n divides $q^m - 1 = \left|M^{\times}\right|$, and $M^{\times}$ is cyclic, so it contains a cyclic subgroup H of order n.
- But then $x \in H \implies p(x) \coloneqq x^n - 1 = 0$, and since $p(x)$ has at most n roots in a field.
- So $H = \left\{ x \in M \;\middle|\; x^n - 1 = 0 \right\}$, i.e. H contains all solutions to $x^n - 1$ in $E[x]$.
- But ζ is one such solution, so $\zeta \in H \subset M^{\times} \subset M$.
- Since $F[\zeta]$ is the smallest field extension containing ζ, we must have $F = M$, so $\ell = 1$, and $k = m$.

■

8.4.3 Spring 2019 #2 ✨

Let $F = \mathbb{F}_p$, where p is a prime number.

a. Show that if $\pi(x) \in F[x]$ is irreducible of degree d, then $\pi(x)$ divides $x^{p^d} - x$.

b. Show that if $\pi(x) \in F[x]$ is an irreducible polynomial that divides $x^{p^n} - x$, then $\deg \pi(x)$ divides n.

Concepts Used:

- Go to a field extension.
  - Orders of multiplicative groups for finite fields are known.
- $\mathbb{GF}(p^n)$ is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.
- $x^{p^d} - x \mid x^{p^n} - x \iff d \mid n$
- $\mathbb{GF}(p^d) \leq \mathbb{GF}(p^n) \iff d \mid n$
- $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n.

Solution:

Proof (of a).

We can consider the quotient $K = \dfrac{\mathbb{F}_p[x]}{\langle \pi(x) \rangle}$, which since $\pi(x)$ is irreducible is an extension of $\mathbb{F}_p$ of degree d and thus a field of size p^d with a natural quotient map of rings $\rho : \mathbb{F}_p[x] \to K$.
Since $K^\times$ is a group of size $p^d - 1$, we know that for any $y \in K^\times$, we have by Lagrange's theorem that the order of y divides $p^d - 1$ and so $y^{p^d} = y$.
So every element in K is a root of $q(x) = x^{p^d} - x$.
Since ρ is a ring morphism, we have

$$\begin{aligned} \rho(q(x)) = \rho(x^{p^d} - x) = \rho(x)^{p^d} - \rho(x) = 0 \in K \\ \iff q(x) \in \ker \rho \\ \iff q(x) \in \langle \pi(x) \rangle \\ \iff \pi(x) \mid q(x) = x^{p^d} - x, \end{aligned}$$

where we've used that "to contain is to divide" in the last step.

■

Proof (of b).

Claim: $\pi(x)$ divides $x^{p^n} - x \iff \deg \pi$ divides n.

Proof (of claim, $\implies$).
Let $L \cong \mathbb{GF}(p^n)$ be the splitting field of $\varphi_n(x) := x^{p^n} - x$; then since $\pi \mid \varphi_n$ by assumption, π splits in L. Let $\alpha \in L$ be any root of π; then there is a tower of extensions $\mathbb{F}_p \leq \mathbb{F}_p(\alpha) \leq L$.
Then $\mathbb{F}_p \leq \mathbb{F}_p(\alpha) \leq L$, and so

$$\begin{aligned} n &= [L : \mathbb{F}_p] \\ &= [L : \mathbb{F}_p(\alpha)]\,[\mathbb{F}_p(\alpha) : \mathbb{F}_p] \\ &= \ell d, \end{aligned}$$

for some $\ell \in \mathbb{Z}^{\geq 1}$, so d divides n.

■

Proof (of claim, $\impliedby$).
$\impliedby$: If $d \mid n$, use the fact (claim) that $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n. So $f = f_i$ for some i.

■

■

8.4.4 ⋆ Fall 2016 #5 🚩

How many monic irreducible polynomials over $\mathbb{F}_p$ of prime degree ℓ are there? Justify your answer.

8.4.5 ⋆ Fall 2013 #7 🚩

Let $F = \mathbb{F}_2$ and let $\overline{F}$ denote its algebraic closure.

a. Show that $\overline{F}$ is not a finite extension of F.

b. Suppose that $\alpha \in \overline{F}$ satisfies $\alpha^{17} = 1$ and $\alpha \neq 1$. Show that $F(\alpha)/F$ has degree 8.

8.5 General Field Extensions

8.5.1 Spring 2020 #3 🚩

Let E be an extension field of F and $\alpha \in E$ be algebraic of odd degree over F.

a. Show that $F(\alpha) = F(\alpha^2)$.

b. Prove that α^{2020} is algebraic of odd degree over F.

8.5.2 Spring 2012 #1 🚩

Suppose that $F \subset E$ are fields such that E/F is Galois and $|\mathrm{Gal}(E/F)| = 14$.

a. Show that there exists a unique intermediate field K with $F \subset K \subset E$ such that $[K : F] = 2$.

b. Assume that there are at least two distinct intermediate subfields $F \subset L_1, L_2 \subset E$ with $[L_i : F] = 7$. Prove that $\mathrm{Gal}(E/F)$ is nonabelian.

8.5.3 Spring 2019 #8 ✨

Let $\zeta = e^{2\pi i/8}$.

a. What is the degree of $\mathbb{Q}(\zeta)/\mathbb{Q}$?

b. How many quadratic subfields of $\mathbb{Q}(\zeta)$ are there?

c. What is the degree of $\mathbb{Q}(\zeta, \sqrt[4]{2})$ over $\mathbb{Q}$?

Concepts Used:

- $\zeta_n := e^{\frac{2\pi i}{n}}$, and ζ_n^k is a primitive nth root of unity $\iff$ $\gcd(n,k)=1$
  - In general, ζ_n^k is a primitive $\dfrac{n}{\gcd(n,k)}$th root of unity.
- $\deg \Phi_n(x) = \varphi(n)$
- $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$
  - Proof: for a nontrivial gcd, the possibilities are

$$p, 2p, 3p, 4p, \cdots, p^{k-2}p, p^{k-1}p.$$

- $\mathsf{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/(n)^\times$

Solution:
Let $K = \mathbb{Q}(\zeta)$.

Proof (of a).

- $\zeta := e^{2\pi i/8}$ is a primitive 8th root of unity
- The minimal polynomial of an nth root of unity is the nth cyclotomic polynomial Φ_n
- The degree of the field extension is the degree of Φ_8, which is

$$\varphi(8) = \varphi(2^3) = 2^{3-1}\cdot(2-1) = 4.$$

- So $[\mathbb{Q}(\zeta):\mathbb{Q}] = 4$.

■

Proof (of b).

- $\mathsf{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/(8)^\times \cong \mathbb{Z}/(4)$ by general theory
- $\mathbb{Z}/(4)$ has exactly one subgroup of index 2.
- Thus there is exactly **one** intermediate field of degree 2 (a quadratic extension).

■

Proof (of c).

- Let $L = \mathbb{Q}(\zeta, \sqrt[4]{2})$.
- Note $\mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2})$
  - $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\zeta)$
    - ♢ $\zeta_8^2 = i$, and $\zeta_8 = \sqrt{2}^{-1} + i\sqrt{2}^{-1}$ so $\zeta_8 + \zeta_8^{-1} = 2/\sqrt{2} = \sqrt{2}$.
  - $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(i, \sqrt{2})$:
    - ♢ $\zeta = e^{2\pi i/8} = \sin(\pi/4) + i\cos(\pi/4) = \frac{\sqrt{2}}{2}(1+i)$.
- Thus $L = \mathbb{Q}(i, \sqrt{2})(\sqrt[4]{2}) = \mathbb{Q}(i, \sqrt{2}, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2})$.
  - Uses the fact that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ since $\sqrt[4]{2}^2 = \sqrt{2}$
- Conclude

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2})]\ [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8$$

using the fact that the minimal polynomial of i over any subfield of $\mathbb{R}$ is always $x^2 + 1$, so $\min_{\mathbb{Q}(\sqrt[4]{2})}(i) = x^2 + 1$ which is degree 2.

■

8.5.4 Fall 2017 #3

Let F be a field. Let $f(x)$ be an irreducible polynomial in $F[x]$ of degree n and let $g(x)$ be any polynomial in $F[x]$. Let $p(x)$ be an irreducible factor (of degree m) of the polynomial $f(g(x))$.

Prove that n divides m. Use this to prove that if r is an integer which is not a perfect square, and n is a positive integer then every irreducible factor of $x^{2n} - r$ over $\mathbb{Q}[x]$ has even degree.

8.5.5 Spring 2015 #2

Let $\mathbb{F}$ be a finite field.

a. Give (with proof) the decomposition of the additive group $(\mathbb{F}, +)$ into a direct sum of cyclic groups.

b. The *exponent* of a finite group is the least common multiple of the orders of its elements. Prove that a finite abelian group has an element of order equal to its exponent.

c. Prove that the multiplicative group $(\mathbb{F}^\times, \cdot)$ is cyclic.

8.5.6 Spring 2014 #3 🚩

Let $F \subset C$ be a field extension with C algebraically closed.

a. Prove that the intermediate field $C_{\text{alg}} \subset C$ consisting of elements algebraic over F is algebraically closed.

b. Prove that if $F \to E$ is an algebraic extension, there exists a homomorphism $E \to C$ that is the identity on F.

9 Modules

9.1 General Questions

9.2 Spring 2017 #3 🚩

Let R be a commutative ring with 1. Suppose that M is a free R-module with a finite basis X.

a. Let $I \trianglelefteq R$ be a proper ideal. Prove that M/IM is a free R/I-module with basis X', where X' is the image of X under the canonical map $M \to M/IM$.

b. Prove that any two bases of M have the same number of elements. You may assume that the result is true when R is a field.

9.3 Spring 2020 #5 ✨

Let R be a ring and $f : M \to N$ and $g : N \to M$ be R-module homomorphisms such that $g \circ f = \text{id}_M$. Show that $N \cong \operatorname{im} f \oplus \ker g$.

Solution:

- We have the following situation:

$$\begin{tikzcd} M \arrow[r, "f"] & N \arrow[l, bend right, dashed, "g"'] \end{tikzcd}$$

Link to Diagram

- Claim: $\operatorname{im} f + \ker g \subseteq N$, and this is in fact an equality.
  - For $n \in N$, write
    $$n = n + (f \circ g)(n) - (f \circ g)(n) = (n - (f \circ g)(n)) + (f \circ g)(n).$$
  - The first term is in $\ker g$:
    $$\begin{aligned} g\left(n - (f \circ g)(n)\right) &= g(n) - (g \circ f \circ g)(n) \\ &= g(n) - (\mathrm{id}_N \circ g)(n) \\ &= g(n) - g(n) \\ &= 0. \end{aligned}$$
  - The second term is clearly in $\operatorname{im} f$.
- Claim: the sum is direct.
  - Suppose $n \in \ker(g) \cap \operatorname{im}(f)$, so $g(n) = 0$ and $n = f(m)$ for some $m \in M$. Then
    $$0 = g(n) = g(f(m)) = (g \circ f)(m) = \mathrm{id}_M(m) = m,$$
    so $m = 0$ and since f is a morphism in R-modules, $n := f(m) = 0$.

9.3.1 Fall 2018 #6 ✨

Let R be a commutative ring, and let M be an R-module. An R-submodule N of M is maximal if there is no R-module P with $N \subsetneq P \subsetneq M$.

a. Show that an R-submodule N of M is maximal $\iff$ M/N is a simple R-module: i.e., M/N is nonzero and has no proper, nonzero R-submodules.

b. Let M be a $\mathbb{Z}$-module. Show that a $\mathbb{Z}$-submodule N of M is maximal $\iff$ $\#M/N$ is a prime number.

c. Let M be the $\mathbb{Z}$-module of all roots of unity in $\mathbb{C}$ under multiplication. Show that there is no maximal $\mathbb{Z}$-submodule of M.

Concepts Used:

- Todo

Solution:

Proof (of a).
By the correspondence theorem, submodules of M/N biject with submodules A of M containing N.
So

- M is maximal:
- $\iff$ no such (proper, nontrivial) submodule A exists
- $\iff$ there are no (proper, nontrivial) submodules of M/N
- $\iff$ M/N is simple.

■

Proof (of b).
Identify $\mathbb{Z}$-modules with abelian groups, then by (a), N is maximal $\iff$ M/N is simple $\iff$ M/N has no nontrivial proper subgroups.

By Cauchy's theorem, if $|M/N| = ab$ is a composite number, then $a \mid ab \implies$ there is an element (and thus a subgroup) of order a. In this case, M/N contains a nontrivial proper cyclic subgroup, so M/N is not simple. So $|M/N|$ can not be composite, and therefore must be prime.

■

Proof (of c).

- Let $G = \left\{ x \in \mathbb{C} \;\middle|\; x^n = 1 \text{ for some } n \in \mathbb{N} \right\}$, and suppose $H < G$ is a proper submodule.
- Since $H \neq G$, there is some p and some k such that $\zeta_{p^k} \notin H$.
  - Otherwise, if H contains every ζ_{p^k} it contains every ζ_n

Then there must be a prime p such that the $\zeta_{p^k} \notin H$ for all k greater than some constant m – otherwise, we can use the fact that if $\zeta_{p^k} \in H$ then $\zeta_{p^\ell} \in H$ for all $\ell \leq k$, and if $\zeta_{p^k} \in H$ for all p and all k then $H = G$.
But this means there are infinitely many elements in $G \setminus H$, and so $\infty = [G : H] = |G/H|$ is not a prime. Thus by (b), H can not be maximal, a contradiction.

■

9.3.2 Fall 2019 Final #2 🚩

Consider the $\mathbb{Z}$-submodule N of $\mathbb{Z}^3$ spanned by

$$\begin{aligned} f_1 &= [-1, 0, 1], \\ f_2 &= [2, -3, 1], \\ f_3 &= [0, 3, 1], \\ f_4 &= [3, 1, 5]. \end{aligned}$$

Find a basis for N and describe $\mathbb{Z}^3/N$.

9.3.3 Spring 2018 #6 🚩

Let

$$\begin{aligned} M &= \{(w, x, y, z) \in \mathbb{Z}^4 \mathrel{\Big|} w + x + y + z \in 2\mathbb{Z}\} \\ N &= \left\{(w, x, y, z) \in \mathbb{Z}^4 \mathrel{\Big|} 4 \mid (w - x),\ 4 \mid (x - y),\ 4 \mid (y - z)\right\}. \end{aligned}$$

a. Show that N is a $\mathbb{Z}$-submodule of M .

b. Find vectors $u_1, u_2, u_3, u_4 \in \mathbb{Z}^4$ and integers d_1, d_2, d_3, d_4 such that

$$\begin{aligned} \{u_1, u_2, u_3, u_4\} & \qquad \text{is a free basis for } M \\ \{d_1u_1,\ d_2u_2,\ d_3u_3,\ d_4u_4\} & \qquad \text{is a free basis for } N \end{aligned}$$

c. Use the previous part to describe M/N as a direct sum of cyclic $\mathbb{Z}$-modules.

9.3.4 Spring 2018 #7 🚩

Let R be a PID and M be an R-module. Let p be a prime element of R. The module M is called $\langle p \rangle$ *-primary* if for every $m \in M$ there exists $k > 0$ such that $p^k m = 0$.

a. Suppose M is $\langle p \rangle$ -primary. Show that if $m \in M$ and $t \in R$, $t \notin \langle p \rangle$, then there exists $a \in R$ such that $atm = m$.

b. A submodule S of M is said to be *pure* if $S \cap rM = rS$ for all $r \in R$. Show that if M is $\langle p \rangle$ -primary, then S is pure if and only if $S \cap p^k M = p^k S$ for all $k \geq 0$.

9.3.5 Fall 2016 #6 🚩

Let R be a ring and $f : M \to N$ and $g : N \to M$ be R-module homomorphisms such that $g \circ f = \mathrm{id}_M$. Show that $N \cong \operatorname{im} f \oplus \ker g$.

9.3.6 Spring 2016 #4 🚩

Let R be a ring with the following commutative diagram of R-modules, where each row represents a short exact sequence of R-modules:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0
\end{tikzcd}$$

Prove that if α and γ are isomorphisms then β is an isomorphism.

9.3.7 Spring 2015 #8 🚩

Let R be a PID and M a finitely generated R-module.

a. Prove that there are R-submodules

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

such that for all $0 \leq i \leq n-1$, the module M_{i+1}/M_i is cyclic.

b. Is the integer n in part (a) uniquely determined by M? Prove your answer.

9.3.8 Fall 2012 #6 🚩

Let R be a ring and M an R-module. Recall that M is *Noetherian* iff any strictly increasing chain of submodule $M_1 \subsetneq M_2 \subsetneq \cdots$ is finite. Call a proper submodule $M' \subsetneq M$ *intersection-decomposable* if it can not be written as the intersection of two proper submodules $M' = M_1 \cap M_2$ with $M_i \subsetneq M$.

Prove that for every Noetherian module M, any proper submodule $N \subsetneq M$ can be written as a finite intersection $N = N_1 \cap \cdots \cap N_k$ of intersection-indecomposable modules.

9.3.9 Fall 2019 Final #1 🚩

Let A be an abelian group, and show A is a $\mathbb{Z}$-module in a unique way.

9.3.10 Fall 2020 #6 🚩

Let R be a ring with 1 and let M be a left R-module. If I is a left ideal of R, define

$$IM := \left\{ \sum_{i=1}^{N<\infty} a_i m_i \;\middle|\; a_i \in I, m_i \in M, n \in \mathbb{N} \right\},$$

i.e. the set of finite sums of of elements of the form am where $a \in I, m \in M$.

a. Prove that $IM \leq M$ is a submodule.

b. Let M, N be left R-modules, I a nilpotent left ideal of R, and $f : M \to N$ an R-module morphism. Prove that if the induced morphism $\overline{f} : M/IM \to N/IN$ is surjective, then f is surjective.

9.4 Torsion and the Structure Theorem

9.4.1 ⋆ Fall 2019 #5 ✨

Let R be a ring and M an R-module.

> *Recall that the set of torsion elements in M is defined by*
>
> $$\mathrm{Tor}(M) = \{m \in M \mid \exists r \in R,\; r \neq 0,\; rm = 0\}.$$

a. Prove that if R is an integral domain, then $\mathrm{Tor}(M)$ is a submodule of M .

b. Give an example where $\mathrm{Tor}(M)$ is not a submodule of M.

c. If R has zero-divisors, prove that every non-zero R-module has non-zero torsion elements.

Concepts Used:

- One-step submodule test.

Solution:

Proof (of a).
It suffices to show that

$$r \in R,\ t_1, t_2 \in \operatorname{Tor}(M) \implies rt_1 + t_2 \in \operatorname{Tor}(M).$$

We have

$$\begin{aligned} t_1 \in \operatorname{Tor}(M) &\implies \exists s_1 \neq 0 \text{ such that } s_1 t_1 = 0 \\ t_2 \in \operatorname{Tor}(M) &\implies \exists s_2 \neq 0 \text{ such that } s_2 t_2 = 0. \end{aligned}$$

Since R is an integral domain, $s_1 s_2 \neq 0$. Then

$$\begin{aligned} s_1 s_2 (rt_1 + t_2) &= s_1 s_2 r t_1 + s_1 s_2 t_2 \\ &= s_2 r(s_1 t_1) + s_1(s_2 t_2) \quad \text{since } R \text{ is commutative} \\ &= s_2 r(0) + s_1(0) \\ &= 0. \end{aligned}$$

■

Proof (of b).
Let $R = \mathbb{Z}/6\mathbb{Z}$ as a $\mathbb{Z}/6\mathbb{Z}$-module, which is not an integral domain as a ring.
Then $[3]_6 \curvearrowright [2]_6 = [0]_6$ and $[2]_6 \curvearrowright [3]_6 = [0]_6$, but $[2]_6 + [3]_6 = [5]_6$, where 5 is coprime to 6, and thus $[n]_6 \curvearrowright [5]_6 = [0] \implies [n]_6 = [0]_6$. So $[5]_6$ is *not* a torsion element.
So the set of torsion elements are not closed under addition, and thus not a submodule.
■

Proof (of c).
Suppose R has zero divisors $a, b \neq 0$ where $ab = 0$. Then for any $m \in M$, we have $b \curvearrowright m := bm \in M$ as well, but then

$$a \curvearrowright bm = (ab) \curvearrowright m = 0 \curvearrowright m = 0_M,$$

so m is a torsion element for any m.
■

9.4.2 ⋆ Spring 2019 #5 ✨

Let R be an integral domain. Recall that if M is an R-module, the *rank* of M is defined to be the maximum number of R-linearly independent elements of M .

a. Prove that for any R-module M, the rank of $\operatorname{Tor}(M)$ is 0.

b. Prove that the rank of M is equal to the rank of of $M/\operatorname{Tor}(M)$.

c. Suppose that M is a non-principal ideal of R.

Prove that M is torsion-free of rank 1 but not free.

Concepts Used:

- Todo

Solution:

Proof (of a).

- Suppose toward a contradiction $\operatorname{Tor}(M)$ has rank $n \geq 1$.
- Then $\operatorname{Tor}(M)$ has a linearly independent generating set $B = \{\mathbf{r}_1, \cdots, \mathbf{r}_n\}$, so in particular

$$\sum_{i=1}^{n} s_i \mathbf{r}_i = 0 \implies s_i = 0_R \, \forall i.$$

- Let $\mathbf{r}$ be any of of these generating elements.
- Since $\mathbf{r} \in \operatorname{Tor}(M)$, there exists an $s \in R \setminus 0_R$ such that $s\mathbf{r} = 0_M$.
- Then $s\mathbf{r} = 0$ with $s \neq 0$, so $\{\mathbf{r}\} \subseteq B$ is *not* a linearly independent set, a contradiction.

■

Proof (of b).

- Let $n = \operatorname{rank} M$, and let $\mathcal{B} = \{\mathbf{r}_i\}_{i=1}^n \subseteq R$ be a generating set.
- Let $\tilde{M} := M / \operatorname{Tor}(M)$ and $\pi : M \to M'$ be the canonical quotient map.

Claim:

$$\tilde{\mathcal{B}} := \pi(\mathcal{B}) = \{\mathbf{r}_i + \operatorname{Tor}(M)\}$$

is a basis for $\tilde{M}$.

Note that the proof follows immediately.

■

Proof (of claim: linearly independent).

- Suppose that

$$\sum_{i=1}^{n} s_i(\mathbf{r}_i + \text{Tor}(M)) = \mathbf{0}_{\tilde{M}}.$$

- Then using the definition of coset addition/multiplication, we can write this as

$$\sum_{i=1}^{n} (s_i\mathbf{r}_i + \text{Tor}(M)) = \left(\sum_{i=1}^{n} s_i\mathbf{r}_i\right) + \text{Tor}(M) = 0_{\tilde{M}}.$$

- Since $\tilde{\mathbf{x}} = 0 \in \tilde{M} \iff \tilde{\mathbf{x}} = \mathbf{x} + \text{Tor}(M)$ where $\mathbf{x} \in \text{Tor}(M)$, this forces $\sum s_i\mathbf{r}_i \in \text{Tor}(M)$.
- Then there exists a scalar $\alpha \in R^{\bullet}$ such that $\alpha \sum s_i\mathbf{r}_i = 0_M$.
- Since R is an integral domain and $\alpha \neq 0$, we must have $\sum s_i\mathbf{r}_i = 0_M$.
- Since $\{\mathbf{r}_i\}$ was linearly independent in M, we must have $s_i = 0_R$ for all i.

■

Proof (of claim: spanning).

- Write $\pi(\mathcal{B}) = \{\mathbf{r}_i + \text{Tor}(M)\}_{i=1}^{n}$ as a set of cosets.
- Letting $\mathbf{x} \in M'$ be arbitrary, we can write $\mathbf{x} = \mathbf{m} + \text{Tor}(M)$ for some $\mathbf{m} \in M$ where $\pi(\mathbf{m}) = \mathbf{x}$ by surjectivity of π.
- Since $\mathcal{B}$ is a basis for M, we have $\mathbf{m} = \sum_{i=1}^{n} s_i\mathbf{r}_i$, and so

$$\begin{aligned}
\mathbf{x} &= \pi(\mathbf{m}) \\
&:= \pi\left(\sum_{i=1}^{n} s_i\mathbf{r}_i\right) \\
&= \sum_{i=1}^{n} s_i\pi(\mathbf{r}_i) \quad \text{since } \pi \text{ is an } R\text{-module morphism} \\
&:= \sum_{i=1}^{n} s_i(\mathbf{r}_i + \text{Tor}(M)),
\end{aligned}$$

which expresses $\mathbf{x}$ as a linear combination of elements in $\mathcal{B}'$.

■

Proof (of c).

Notation: Let 0_R denote $0 \in R$ regarded as a ring element, and $\mathbf{0} \in R$ denoted 0_R regarded as a module element (where R is regarded as an R-module over itself)

Proof (that M is not free).

- **Claim**: If $I \subseteq R$ is an ideal *and* a free R-module, then I is principal .
  - Suppose I is free and let $I = \langle B \rangle$ for some basis, we will show $|B| = 1>$
  - Toward a contradiction, suppose $|B| \geq 2$ and let $m_1, m_2 \in B$.
  - Then since R is commutative, $m_2 m_1 - m_1 m_2 = 0$ and this yields a linear dependence
  - So B has only one element m.
  - But then $I = \langle m \rangle = R_m$ is cyclic as an R- module and thus principal as an ideal of R.
  - Now since M was assumed to *not* be principal, M is not free (using the contrapositive of the claim).

■

Proof (that M is rank 1).

- For any module, we can take an element $\mathbf{m} \in M^\bullet$ and consider the cyclic submodule $R\mathbf{m}$.
- Since M is not principle, it is not the zero ideal, and contains at least two elements. So we can consider an element $\mathbf{m} \in M$.
- We have $\operatorname{rank}_R(M) \geq 1$, since $R\mathbf{m} \leq M$ and $\{m\}$ is a subset of some spanning set.
- $R\mathbf{m}$ can not be linearly dependent, since R is an integral domain and $M \subsetneq R$, so $\alpha\mathbf{m} = \mathbf{0} \implies \alpha = 0_R$.
- Claim: since R is commutative, $\operatorname{rank}_R(M) \leq 1$.
  - If we take two elements $\mathbf{m}, \mathbf{n} \in M^\bullet$, then since $m, n \in R$ as well, we have $nm = mn$ and so

$$(n)\mathbf{m} + (-m)\mathbf{n} = 0_R = \mathbf{0}$$

  is a linear dependence.

M **is torsion-free**:

- Let $\mathbf{x} \in \operatorname{Tor} M$, then there exists some $r \neq 0 \in R$ such that $r\mathbf{x} = \mathbf{0}$.
- But $\mathbf{x} \in R$ as well and R is an integral domain, so $\mathbf{x} = 0_R$, and thus $\operatorname{Tor}(M) = \{0_R\}$.

■

■

9.4.3 ⋆ Spring 2020 #6 ✨

Let R be a ring with unity.

a. Give a definition for a free module over R.

b. Define what it means for an R-module to be torsion free.

c. Prove that if F is a free module, then any short exact sequence of R-modules of the following form splits:

$$0 \to N \to M \to F \to 0.$$

d. Let R be a PID. Show that any finitely generated R-module M can be expressed as a direct sum of a torsion module and a free module.

You may assume that a finitely generated torsionfree module over a PID is free.

Solution:
Let R be a ring with 1.

Proof (of a).
An R-module M is **free** if any of the following conditions hold:

- M admits an R-linearly independent spanning set $\{\mathbf{b}_\alpha\}$, so

  $$m \in M \implies m = \sum_\alpha r_\alpha \mathbf{b}_\alpha$$

  and

  $$\sum_\alpha r_\alpha \mathbf{b}_\alpha = 0_M \implies r_\alpha = 0_R$$

  for all α.
- M admits a decomposition $M \cong \bigoplus_\alpha R$ as a direct sum of R-submodules.
- There is a nonempty set X an monomorphism $X \hookrightarrow M$ of sets such that for every R-module N, every set map $X \to N$ lifts to a unique R-module morphism $M \to N$, so the following diagram commutes:

  $$\begin{tikzcd} M \arrow[dr, dotted, "\exists ! \tilde{f}"] & \\ X \arrow[u, hook] \arrow[r, "f"] & N \end{tikzcd}$$

Equivalently,

$$\underset{\mathsf{Set}}{\operatorname{Hom}}(X, \operatorname{Forget}(N)) \xrightarrow{\sim} \underset{\mathsf{R\text{-}Mod}}{\operatorname{Hom}}(M, N).$$

■

Proof (of b).

- Define the annihilator:

  $$\operatorname{Ann}(m) := \left\{ r \in R \;\middle|\; r \cdot m = 0_M \right\} \trianglelefteq R.$$

  - Note that $mR \cong R/\operatorname{Ann}(m)$.
- Define the torsion submodule:

  $$M_t := \left\{ m \in M \;\middle|\; \operatorname{Ann}(m) \neq 0 \right\} \leq M$$

- M is **torsionfree** iff $M_t = 0$ is the trivial submodule.

■

Proof (of c).

- Let the following be an SES where F is a free R-module:

$$0 \to N \to M \xrightarrow{\pi} F \to 0.$$

- Since F is free, there is a generating set $X = \{x_\alpha\}$ and a map $\iota : X \hookrightarrow F$ satisfying the 3rd property from (a).
  - If we construct any map $f : X \to M$, the universal property modules will give a lift $\tilde{f} : F \to M$
- Identify X with $\iota(X) \subseteq F$.
- For every $x \in X$, the preimage $\pi^{-1}(x)$ is nonempty by surjectivity. So arbitrarily pick any preimage.
- $\{\iota(x_\alpha)\} \subseteq F$ and π is surjective, so choose fibers $\{y_\alpha\} \subseteq M$ such that $\pi(y_\alpha) = \iota(x_\alpha)$ and define

$$\begin{aligned} f : X &\to M \\ x_\alpha &\mapsto y_\alpha. \end{aligned}$$

- The universal property yields $h : F \to M$:

$$\begin{tikzcd}
 & & & X = \{x_\alpha\} \arrow[ld, "f"'] \arrow[d, hook, "\iota"] & \\
0 \arrow[r] & N \arrow[r] & M \arrow[r, "\pi"'] & F \arrow[r] \arrow[l, dotted, bend right, "\exists ! h"'] & 0
\end{tikzcd}$$

- It remains to check that it's a section.
  - Write $f = \sum r_i x_i$, then since both maps are R-module morphism, by R-linearity we can write

$$\begin{aligned} (\pi \circ h)(f) &= (\pi \circ h)\left(\sum r_i x_i\right) \\ &= \sum r_i (\pi \circ h)(x_i), \end{aligned}$$

  but since $h(x_i) \in \pi^{-1}(x_i)$, we have $(\pi \circ h)(x_i) = x_i$. So this recovers f.

■

Proof (of c, shorter proof).

- Free implies projective
  - Universal property of **projective** objects: for every epimorphism $\pi : M \twoheadrightarrow N$ and every $f : P \to N$ there exists a unique lift $\tilde{f} : P \to M$:

$$\begin{tikzcd}
 & P \arrow[d, "f"] \arrow[dl, dotted, "\exists ! \tilde{f}"'] \\
M \arrow[r, "\pi"] & N
\end{tikzcd}$$

  - Construct φ in the following diagram using the same method as above (surjectivity to pick elements in preimage):

$$\begin{tikzcd}
 & X \arrow[d, hook, "\iota"] \arrow[ddl, bend right, "\varphi"'] & \\
 & F \arrow[d, "f"] \arrow[dl, dashed, "\exists \tilde{\varphi}"'] & \\
M \arrow[r, two heads, "\pi"'] & N \arrow[r] & 0
\end{tikzcd}$$

Link to Diagram

- Now take the identity map, then commutativity is equivalent to being a section.

$$\begin{tikzcd}
 & & & F \arrow[d, "\mathbb{1}_F"] \arrow[dl, "\exists ! h"'] & \\
0 \arrow[r] & N \arrow[r] & M \arrow[r] & F \arrow[r] & 0
\end{tikzcd}$$

■

Proof (of d).
There is a SES

$$0 \longrightarrow M_t \longrightarrow M \longrightarrow M/M_t \longrightarrow 0$$

Claim: M/M_t is a free R-module, so this sequence splits and $M \cong M_t \oplus \frac{M}{M_t}$, where M_t is a torsion R-module.

Note that by the hint, since R is a PID, it suffices to show that M/M_t is torsionfree.

- Let $m + M_t \in M/M_t$ be arbitrary. Suppose this is a torsion element, the claim is that it must be the trivial coset. This will follow if $m \in M_t$
- Since this is torsion, there exists $r \in R$ such that

$$M_t = r(m + M_t) := (rm) + M_t \implies rm \in M_t.$$

- Then rm is torsion in M, so there exists some $s \in R$ such $s(rm) = 0_M$.
- Then $(sr)m = 0_M$ which forces $m \in M_t$

■

9.4.4 Spring 2012 #5

Let M be a finitely generated module over a PID R.

a. M_t be the set of torsion elements of M, and show that M_t is a submodule of M.

b. Show that M/M_t is torsion free.

c. Prove that $M \cong M_t \oplus F$ where F is a free module.

9.4.5 Spring 2017 #5

Let R be an integral domain and let M be a nonzero torsion R-module.

a. Prove that if M is finitely generated then the annihilator in R of M is nonzero.

b. Give an example of a non-finitely generated torsion R-module whose annihilator is (0), and justify your answer.

9.4.6 Fall 2019 Final #3

Let $R = k[x]$ for k a field and let M be the R-module given by

$$M = \frac{k[x]}{(x-1)^3} \oplus \frac{k[x]}{(x^2+1)^2} \oplus \frac{k[x]}{(x-1)\left(x^2+1\right)^4} \oplus \frac{k[x]}{(x+2)\left(x^2+1\right)^2}.$$

Describe the elementary divisors and invariant factors of M.

9.4.7 Fall 2019 Final #4

Let $I = (2, x)$ be an ideal in $R = \mathbb{Z}[x]$, and show that I is not a direct sum of nontrivial cyclic R-modules.

9.4.8 Fall 2019 Final #5

Let R be a PID.

a. Classify irreducible R-modules up to isomorphism.

b. Classify indecomposable R-modules up to isomorphism.

9.4.9 Fall 2019 Final #6

Let V be a finite-dimensional k-vector space and $T : V \to V$ a non-invertible k-linear map. Show that there exists a k-linear map $S : V \to V$ with $T \circ S = 0$ but $S \circ T \neq 0$.

9.4.10 Fall 2019 Final #7

Let $A \in M_n(\mathbb{C})$ with $A^2 = A$. Show that A is similar to a diagonal matrix, and exhibit an explicit diagonal matrix similar to A.

9.4.11 Fall 2019 Final #10

Show that the eigenvalues of a Hermitian matrix A are real and that $A = PDP^{-1}$ where P is an invertible matrix with orthogonal columns.

9.4.12 Fall 2020 #7

Let $A \in \operatorname{Mat}(n \times n, \mathbb{R})$ be arbitrary. Make $\mathbb{R}^n$ into an $\mathbb{R}[x]$-module by letting $f(x).\mathbf{v} := f(A)(\mathbf{v})$ for $f(\mathbf{v}) \in \mathbb{R}[x]$ and $\mathbf{v} \in \mathbb{R}^n$. Suppose that this induces the following direct sum decomposition:

$$\mathbb{R}^n \cong \frac{\mathbb{R}[x]}{\langle (x-1)^3 \rangle} \oplus \frac{\mathbb{R}[x]}{\langle (x^2+1)^2 \rangle} \oplus \frac{\mathbb{R}[x]}{\langle (x-1)(x^2-1)(x^2+1)^4 \rangle} \oplus \frac{\mathbb{R}[x]}{\langle (x+2)(x^2+1)^2 \rangle}.$$

a. Determine the elementary divisors and invariant factors of A.

b. Determine the minimal polynomial of A.

c. Determine the characteristic polynomial of A.

10 Linear Algebra: Diagonalizability

10.1 Fall 2017 #7

Let F be a field and let V and W be vector spaces over F .

Make V and W into $F[x]$-modules via linear operators T on V and S on W by defining $X \cdot v = T(v)$ for all $v \in V$ and $X \cdot w = S(w)$ for all w ∈ W .

Denote the resulting $F[x]$-modules by V_T and W_S respectively.

a. Show that an $F[x]$-module homomorphism from V_T to W_S consists of an F-linear transformation $R : V \to W$ such that $RT = SR$.

b. Show that $VT \cong WS$ as $F[x]$-modules $\iff$ there is an F-linear isomorphism $P : V \to W$ such that $T = P^{-1}SP$.

c. Recall that a module M is *simple* if $M \neq 0$ and any proper submodule of M must be zero. Suppose that V has dimension 2. Give an example of F, T with V_T simple.

d. Assume F is algebraically closed. Prove that if V has dimension 2, then any V_T is not simple.

10.2 Spring 2015 #3

Let F be a field and V a finite dimensional F-vector space, and let $A, B : V \to V$ be commuting F-linear maps. Suppose there is a basis $\mathcal{B}_1$ with respect to which A is diagonalizable and a basis $\mathcal{B}_2$ with respect to which B is diagonalizable.

Prove that there is a basis $\mathcal{B}_3$ with respect to which A and B are both diagonalizable.

10.3 Fall 2016 #2 🚩

Let A, B be two $n \times n$ matrices with the property that $AB = BA$. Suppose that A and B are diagonalizable. Prove that A and B are *simultaneously* diagonalizable.

10.4 Spring 2019 #1 ✨

Let A be a square matrix over the complex numbers. Suppose that A is nonsingular and that A^{2019} is diagonalizable over $\mathbb{C}$.

Show that A is also diagonalizable over $\mathbb{C}$.

Concepts Used:

- A is diagonalizable iff $\min_A(x)$ is separable.
  - See further discussion here.

Solution:

Claim: If $A \in \mathrm{GL}(m, \mathbb{F})$ is invertible and $A^n/\mathbb{F}$ is diagonalizable, then $A/\mathbb{F}$ is diagonalizable.

Proof (of claim).

- Let $A \in \mathrm{GL}(m, \mathbb{F})$.
- Since A^n is diagonalizable, $\min_{A^n}(x) \in \mathbb{F}[x]$ is separable and thus factors as a product of m **distinct** linear factors:

$$\min_{A^n}(x) = \prod_{i=1}^{m}(x - \lambda_i), \quad \min_{A^n}(A^n) = 0$$

  where $\{\lambda_i\}_{i=1}^m \subset \mathbb{F}$ are the **distinct** eigenvalues of A^n.

- Moreover $A \in \mathrm{GL}(m, \mathbb{F}) \implies A^n \in \mathrm{GL}(m, \mathbb{F})$: A is invertible $\iff \det(A) = d \in \mathbb{F}^\times$, and so $\det(A^n) = \det(A)^n = d^n \in \mathbb{F}^\times$ using the fact that the determinant is a ring morphism $\det : \mathrm{Mat}(m \times m) \to \mathbb{F}$ and $\mathbb{F}^\times$ is closed under multiplication.
- So A^n is invertible, and thus has trivial kernel, and thus zero is not an eigenvalue, so $\lambda_i \neq 0$ for any i.
- Since the λ_i are distinct and nonzero, this implies x^k is not a factor of $\mu_{A^n}(x)$ for any $k \geq 0$. Thus the m terms in the product correspond to precisely m **distinct linear** factors.
- We can now construct a polynomial that annihilates A, namely

$$q_A(x) := \min_{A^n}(x^n) = \prod_{i=1}^{m}(x^n - \lambda_i) \in \mathbb{F}[x],$$

  where we can note that $q_A(A) = \min_{A^n}(A^n) = 0$, and so $\min_A(x) \mid q_A(x)$ by minimality.

Claim: $q_A(x)$ has exactly nm distinct linear factors in $\overline{\mathbb{F}}[x]$

- This reduces to showing that no pair $x^n - \lambda_i, x^n - \lambda_j$ share a root. and that $x^n - \lambda_i$ does not have multiple roots.
- For the first claim, we can factor

$$x^n - \lambda_i = \prod_{k=1}^{n}(x - \lambda_i^{\frac{1}{n}} e^{\frac{2\pi i k}{n}}) := \prod_{k=1}^{n}(x - \lambda^{\frac{1}{n}} \zeta_n^k),$$

  where we now use the fact that $i \neq j \implies \lambda_i^{\frac{1}{n}} \neq \lambda_j^{\frac{1}{n}}$. Thus no term in the above product appears as a factor in $x^n - \lambda_j$ for $j \neq i$.

- For the second claim, we can check that $\frac{\partial}{\partial x}(x^n - \lambda_i) = nx^{n-1} \neq 0 \in \mathbb{F}$, and $\gcd(x^n - \lambda_i, nx^{n-1}) = 1$ since the latter term has only the roots $x = 0$ with multiplicity $n - 1$, whereas $\lambda_i \neq 0 \implies$ zero is not a root of $x^n - \lambda_i$.

But now since $q_A(x)$ has exactly distinct linear factors in $\overline{\mathbb{F}}[x]$ and $\min_A(x) \mid q_A(x)$, $\min_A(x) \in \mathbb{F}[x]$ can only have distinct linear factors, and A is thus diagonalizable over $\mathbb{F}$. ■

11 Linear Algebra: Misc

11.1 ⋆ Spring 2012 #6

Let k be a field and let the group $G = \mathrm{GL}(m, k) \times \mathrm{GL}(n, k)$ acts on the set of $m \times n$ matrices $M_{m,n}(k)$ as follows:

$$(A, B) \cdot X = AXB^{-1}$$

where $(A, B) \in G$ and $X \in M_{m,n}(k)$.

a. State what it means for a group to act on a set. Prove that the above definition yields a group action.

b. Exhibit with justification a subset S of $M_{m,n}(k)$ which contains precisely one element of each orbit under this action.

11.2 ⋆ Spring 2014 #7

Let $G = \mathrm{GL}(3, \mathbb{Q}[x])$ be the group of invertible 3×3 matrices over $\mathbb{Q}[x]$. For each $f \in \mathbb{Q}[x]$, let S_f be the set of 3×3 matrices A over $\mathbb{Q}[x]$ such that $\det(A) = cf(x)$ for some nonzero constant $c \in \mathbb{Q}$.

a. Show that for $(P, Q) \in G \times G$ and $A \in S_f$, the formula

$$(P, Q) \cdot A := PAQ^{-1}$$

gives a well defined map $G \times G \times S_f \to S_f$ and show that this map gives a group action of $G \times G$ on S_f.

b. For $f(x) = x^3(x^2 + 1)^2$, give one representative from each orbit of the group action in (a), and justify your assertion.

11.3 Fall 2012 #7

Let k be a field of characteristic zero and $A, B \in M_n(k)$ be two square $n \times n$ matrices over k such that $AB - BA = A$. Prove that $\det A = 0$.

Moreover, when the characteristic of k is 2, find a counterexample to this statement.

11.4 Fall 2012 #8

Prove that any nondegenerate matrix $X \in M_n(\mathbb{R})$ can be written as $X = UT$ where U is orthogonal and T is upper triangular.

11.5 Fall 2012 #5

Let U be an infinite-dimensional vector space over a field k, $f : U \to U$ a linear map, and $\{u_1, \cdots, u_m\} \subset U$ vectors such that U is generated by $\left\{u_1, \cdots, u_m, f^d(u_1), \cdots, f^d(u_m)\right\}$ for some $d \in \mathbb{N}$.

Prove that U can be written as a direct sum $U \cong V \oplus W$ such that

1. V has a basis consisting of some vector $v_1, \cdots v_n, f^d(v_1), \cdots, f^d(v_n)$ for some $d \in \mathbb{N}$, and
2. W is finite-dimensional.

Moreover, prove that for any other decomposition $U \cong V' \oplus W'$, one has $W' \cong W$.

11.6 Fall 2015 #7

a. Show that two 3×3 matrices over $\mathbb{C}$ are similar $\iff$ their characteristic polynomials are equal and their minimal polynomials are equal.

b. Does the conclusion in (a) hold for 4×4 matrices? Justify your answer with a proof or counterexample.

11.7 Fall 2014 #4

Let F be a field and T an $n \times n$ matrix with entries in F. Let I be the ideal consisting of all polynomials $f \in F[x]$ such that $f(T) = 0$.

Show that the following statements are equivalent about a polynomial $g \in I$:

a. g is irreducible.

b. If $k \in F[x]$ is nonzero and of degree strictly less than g, then $k[T]$ is an invertible matrix.

11.8 Fall 2015 #8 🚩

Let V be a vector space over a field F and $V^\vee$ its dual. A *symmetric bilinear form* $(-,-)$ on V is a map $V \times V \to F$ satisfying

$$(av_1 + bv_2, w) = a(v_1, w) + b(v_2, w) \quad \text{and} \quad (v_1, v_2) = (v_2, v_1)$$

for all $a, b \in F$ and $v_1, v_2 \in V$. The form is *nondegenerate* if the only element $w \in V$ satisfying $(v, w) = 0$ for all $v \in V$ is $w = 0$.

Suppose $(-,-)$ is a nondegenerate symmetric bilinear form on V. If W is a subspace of V, define

$$W^\perp := \left\{ v \in V \;\middle|\; (v, w) = 0 \text{ for all } w \in W \right\}.$$

a. Show that if X, Y are subspaces of V with $Y \subset X$, then $X^\perp \subseteq Y^\perp$.

b. Define an injective linear map

$$\psi : Y^\perp / X^\perp \hookrightarrow (X/Y)^\vee$$

which is an isomorphism if V is finite dimensional.

11.9 Fall 2018 #4 ✨

Let V be a finite dimensional vector space over a field (the field is not necessarily algebraically closed).

Let $\varphi : V \to V$ be a linear transformation. Prove that there exists a decomposition of V as $V = U \oplus W$, where U and W are φ-invariant subspaces of V , $\varphi|_U$ is nilpotent, and $\varphi|_W$ is nonsingular.

Revisit.

Solution:
Let $m(x)$ be the minimal polynomial of φ. If the polynomial $f(x) = x$ doesn't divide m, then f does not have zero as an eigenvalue, so φ is nonsingular and since 0 is nilpotent, $\varphi + 0$ works.
Otherwise, write $\varphi(x) = x^m \rho(x)$ where $\gcd(x, \rho(x)) = 1$.
Then

$$V \cong \frac{k[x]}{m(x)} \cong \frac{k[x]}{(x^m)} \oplus \frac{k[x]}{(\rho)} := U \oplus W$$

by the Chinese Remainder theorem.
We can now note that $\varphi|_U$ is nilpotent because it has characteristic polynomial x^m, and $\varphi|_W$ is nonsingular since $\lambda = 0$ is not an eigenvalue by construction.

11.10 Fall 2018 #5 ✨

Let A be an $n \times n$ matrix.

a. Suppose that v is a column vector such that the set $\{v, Av, ..., A^{n-1}v\}$ is linearly independent. Show that any matrix B that commutes with A is a polynomial in A.

b. Show that there exists a column vector v such that the set $\{v, Av, ..., A^{n-1}v\}$ is linearly independent $\iff$ the characteristic polynomial of A equals the minimal polynomial of A.

Concepts Used:

- Powers of A commute with polynomials in A.
- The image of a linear map is determined by the image of a basis

Strategy:

- Use Cayley-Hamilton to relate the minimal polynomial to a linear dependence.
- Get a lower bound on the degree of the minimal polynomial.
- Use $A \curvearrowright k[x]$ to decompose into cyclic $k[x]$-modules, and use special form of denominators in the invariant factors.
- Reduce to monomials.

Solution:

Proof (of a).
Letting $\mathbf{v}$ be fixed, since $\left\{A^j\mathbf{v}\right\}$ spans V we have A

$$B\mathbf{v} = \sum_{j=0}^{n-1} c_j A^j \mathbf{v}.$$

So let $p(x) = \sum_{j=0}^{n-1} c_j x^j$. Then consider how B acts on any basis vector $A^k\mathbf{v}$.

We have

$$\begin{aligned} BA^k\mathbf{v} &= A^k B\mathbf{v} \\ &= A^k p(A)\mathbf{v} \\ &= p(A)A^k\mathbf{v}, \end{aligned}$$

so $B = p(A)$ as operators since their actions agree on every basis vector in V. ■

Proof (of b, $\implies$).

- If $\left\{ A^j \mathbf{v}_k \;\middle|\; 0 \leq j \leq n-1 \right\}$ is linearly independent, this means that A does satisfy any polynomial of degree $d < n$.
- So $\deg m_A(x) = n$, and since $m_A(x)$ divides $\chi_A(x)$ and both are monic degree polynomials of degree n, they must be equal.

$\blacksquare$

Proof (of b, $\impliedby$).

- Let $A \curvearrowright k[x]$ by $A \curvearrowright p(x) := p(A)$. This induces an invariant factor decomposition $V =\cong \bigoplus k[x]/(f_i)$.
- Since the product of the invariant factors is the characteristic polynomial, the largest invariant factor is the minimal polynomial, and these two are equal, there can only be one invariant factor and thus the invariant factor decomposition is

  $$V \cong \frac{k[x]}{(\chi_A(x))}$$

  as an isomorphism of $k[x]$-modules.
- So V is a cyclic $k[x]$ module, which means that $V = k[x] \curvearrowright \mathbf{v}$ for some $\mathbf{v} \in V$ such that $\mathrm{Ann}(\mathbf{v}) = \chi_A(x)$, i.e. there is some element $\mathbf{v} \in V$ whose orbit is all of V.
- But then noting that monomials span $k[x]$ as a k-module, we can write

  $$\begin{aligned} V &\cong k[x] \curvearrowright \mathbf{v} \\ &:= \left\{ f(x) \curvearrowright \mathbf{v} \;\middle|\; f \in k[x] \right\} \\ &= \operatorname{span}_k \left\{ x^k \curvearrowright \mathbf{v} \;\middle|\; k \geq 0 \right\} \\ &:= \operatorname{span}_k \left\{ A^k \mathbf{v} \;\middle|\; k \geq 0 \right\}, \end{aligned}$$

  where we've used that x acts by A and thus x^k acts by A^k.
- Moreover, we can note that if $\ell \geq \deg \chi_A(x)$, then A^ℓ is a linear combination of $\left\{ A^j \;\middle|\; 0 \leq j \leq n-1 \right\}$, and so

  $$\begin{aligned} V &\cong \operatorname{span}_k \left\{ A^\ell \mathbf{v} \;\middle|\; \ell \geq 0 \right\} \\ &= \operatorname{span}_k \left\{ A^\ell \mathbf{v} \;\middle|\; 1 \leq \ell \leq n-1 \right\}. \end{aligned}$$

$\blacksquare$

11.11 Fall 2019 #8 🚩

Let $\{e_1, \cdots, e_n\}$ be a basis of a real vector space V and let

$$\Lambda := \left\{ \sum r_i e_i \,\middle|\, r_i \in \mathbb{Z} \right\}$$

Let $\cdot$ be a non-degenerate ($v \cdot w = 0$ for all $w \in V \iff v = 0$) symmetric bilinear form on V such that the Gram matrix $M = (e_i \cdot e_j)$ has integer entries.

Define the dual of Λ to be

$$\Lambda^\vee := \left\{ v \in V \,\middle|\, v \cdot x \in \mathbb{Z} \text{ for all } x \in \Lambda \right\}.$$

a. Show that $\Lambda \subset \Lambda^\vee$.

b. Prove that $\det M \neq 0$ and that the rows of M^{-1} span $\Lambda^\vee$.

c. Prove that $\det M = |\Lambda^\vee / \Lambda|$.

Todo, missing part (c).

Solution:

Proof (of a).

- Let $\mathbf{v} \in \Lambda$, so $\mathbf{v} = \sum_{i=1}^n r_i \mathbf{e}_i$ where $r_i \in \mathbb{Z}$ for all i.
- Then if $\mathbf{x} = \sum_{j=1}^n s_j \mathbf{e}_j \in \Lambda$ is arbitrary, we have $s_j \in \mathbb{Z}$ for all j and

$$\begin{aligned} \langle \mathbf{v}, \ \mathbf{x} \rangle &= \left\langle \sum_{i=1}^n r_i \mathbf{e}_i, \ \sum_{j=1}^n s_j \mathbf{e}_j \right\rangle \\ &= \sum_{i=1}^n \sum_{j=1}^n r_i s_j \langle \mathbf{e}_i, \ \mathbf{e}_j \rangle \in \mathbb{Z} \end{aligned}$$

since this is a sum of products of integers (since $\langle \mathbf{e}_i, \ \mathbf{e}_j \rangle \in \mathbb{Z}$ for each i, j pair by assumption) so $\mathbf{v} \in \Lambda^\vee$ by definition.

■

Proof (of b).

Claim: The determinant is nonzero.

- Suppose $\det M = 0$. Then $\ker M \neq \mathbf{0}$, so let $\mathbf{v} \in \ker M$ be given by $\mathbf{v} = \sum_{i=1}^n v_i \mathbf{e}_i \neq \mathbf{0}$.
- Note that

$$M\mathbf{v} = 0 \implies \begin{bmatrix} \mathbf{e}_1 \cdot \mathbf{e}_1 & \mathbf{e}_1 \cdot \mathbf{e}_2 & \cdots \\ \mathbf{e}_2 \cdot \mathbf{e}_1 & \mathbf{e}_2 \cdot \mathbf{e}_2 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \end{bmatrix} = \mathbf{0}$$

$$\implies \sum_{j=1}^n v_j \langle \mathbf{e}_k,\ \mathbf{e}_j \rangle = 0 \quad \text{foreachfixed} \quad k.$$

- We can now note that $\langle \mathbf{e}_k,\ \mathbf{v} \rangle = \sum_{j=1}^n v_j \langle \mathbf{e}_k,\ \mathbf{e}_j \rangle = 0$ for every k by the above observation, which forces $\mathbf{v} = 0$ by non-degeneracy of $\langle -,\ - \rangle$, a contradiction.

■

Proof (of c).
???

Missing work!

■

Solution (Alternative):
Write $M = A^t A$ where A has the $\mathbf{e}_i$ as columns. Then

$$\begin{aligned} M\mathbf{x} = 0 &\implies A^t A\mathbf{x} = 0 \\ &\implies \mathbf{x}^t A^t A \mathbf{x} = 0 \\ &\implies \|A\mathbf{x}\|^2 = 0 \\ &\implies A\mathbf{x} = 0 \\ &\implies \mathbf{x} = 0, \end{aligned}$$

since A has full rank because the $\mathbf{e}_i$ are linearly independent.
Let $A = [\mathbf{e}_1^t, \cdots, \mathbf{e}_n^t]$ be the matrix with $\mathbf{e}_i$ in the ith column.

Claim: The rows of A^{-1} span $\Lambda^\vee$. Equivalently, the columns of A^{-t} span $\Lambda^\vee$.

- Let $B = A^{-t}$ and let $\mathbf{b}_i$ denote the columns of B, so $\operatorname{im} B = \operatorname{span}\{\mathbf{b}_i\}$.

- Since $A \in \mathrm{GL}(n, \mathbb{Z})$, $A^{-1}, A^t, A^{-t} \in \mathrm{GL}(n, \mathbb{Z})$ as well.

$$\begin{aligned}
\mathbf{v} \in \Lambda^\vee &\implies \langle \mathbf{e}_i,\ \mathbf{v} \rangle = z_i \in \mathbb{Z} \quad \forall i \\
&\implies A^t \mathbf{v} = \mathbf{z} := [z_1, \cdots, z_n] \in \mathbb{Z}^n \\
&\implies \mathbf{v} = A^{-t}\mathbf{z} := B\mathbf{z} \in \operatorname{im} B \\
&\implies \mathbf{v} \in \operatorname{im} B \\
&\implies \Lambda^\vee \subseteq \operatorname{im} B,
\end{aligned}$$

and

$$\begin{aligned}
B^t A = (A^{-t})^t A &= A^{-1} A = I \\
&\implies \mathbf{b}_i \cdot \mathbf{e}_j = \delta_{ij} \in \mathbb{Z} \\
&\implies \operatorname{im} B \subseteq \operatorname{span} \Lambda^\vee.
\end{aligned}$$

11.12 Spring 2013 #6 ✨

Let V be a finite dimensional vector space over a field F and let $T : V \to V$ be a linear operator with characteristic polynomial $f(x) \in F[x]$.

a. Show that $f(x)$ is irreducible in $F[x] \iff$ there are no proper nonzero subspaces $W < V$ with $T(W) \subseteq W$.

b. If $f(x)$ is irreducible in $F[x]$ and the characteristic of F is 0, show that T is diagonalizable when we extend the field to its algebraic closure.

Is there a proof without matrices? What if V is infinite dimensional?

How to extend basis?

Concepts Used:

- Every $\mathbf{v} \in V$ is T-cyclic $\iff$ $\chi_T(x)/\daleth$ is irreducible.
  - $\implies$: Same as argument below.
  - $\impliedby$: Suppose f is irreducible, then f is equal to the minimal polynomial of T.
- Characterization of diagonalizability: T is diagonalizable over F $\iff$ $\min_{T,F}$ is squarefree in $\overline{F}[x]$?

Solution:
Let f be the characteristic polynomial of T.

Proof (of a, $\implies$. Matrix-dependent).
$\implies$:

- By contrapositive, suppose there is a proper nonzero invariant subspace $W < V$ with $T(W) \subseteq W$, we will show the characteristic polynomial $f := \chi_{V,T}(x)$ is reducible.
- Since $T(W) \subseteq W$, the restriction $g := \chi_{V,T}(x) \Big|_W : W \to W$ is a linear operator on W.

Claim: g divides f in $\mathbb{F}[x]$ and $\deg(g) < \deg(f)$.

- Choose an ordered basis for W, say $\mathcal{B}_W := \{\mathbf{w}_1, \cdots, \mathbf{w}_k\}$ where $k = \dim_F(W)$
- Claim: this can be extended to a basis of V, say $\mathcal{B}_V := \{\mathbf{w}_1, \cdots, \mathbf{w}_k, \mathbf{v}_1, \cdots, \mathbf{v}_j\}$ where $k + j = \dim_F(V)$.
  - Note that since $W < V$ is proper, $j \geq 1$.
- Restrict T to W to get T_W, then let $B = [T_W]_{\mathcal{B}_W}$ be the matrix representation of T_W with respect to $\mathcal{B}_W$.
- Now consider the matrix representation $[T]_{\mathcal{B}_V}$, in block form this is given by

  $$[T]_{\mathcal{B}_V} = \begin{bmatrix} B & C \\ 0 & D \end{bmatrix}$$

  where we've used that $W < V$ is proper to get the existence of C, D (there is at least one additional row/column since $j \geq 1$ in the extended basis.)

  Why?

- Now expand along the first column block to obtain

  $$\chi_{T,V}(x) := \det([T]_{\mathcal{B}_V} - xI) = \det(B - xI) \cdot \det(D - xI) := \chi_{T,W}(x) \cdot \det(D - xI).$$

- Claim: $\det(D - xI) \in xF[x]$ is nontrivial
- The claim follows because this forces $\deg(\det(D - xI)) \geq 1$ and so $\chi_{T,W}(x)$ is a proper divisor of $\chi_{T,V}(x)$.
- Thus f is reducible.

■

Proof (of a, $\Longleftarrow$).

$\Longleftarrow$

- Suppose f is reducible, then we will produce a proper T-invariant subspace.
- Claim: if f is reducible, there exists a nonzero, noncyclic vector $\mathbf{v}$.
- Then $\operatorname{span}_k \left\{ T^j \mathbf{v} \right\}_{j=1}^{d}$ is a T-invariant subspace that is nonzero, and not the entire space since $\mathbf{v}$ is not cyclic.

■

Proof (of b).

- Let $\min_{T,F}(x)$ be the minimal polynomial of T and $\chi_{T,F}(x)$ be its characteristic polynomial.
- By Cayley-Hamilton, $\min_{T,F}(x)$ divides $\chi_{T,F}$
- Since $\chi_{T,F}$ is irreducible, these polynomials are equal.
- Claim: T/F is diagonalizable $\iff$ $\min_{T,F}$ splits over F and is squarefree.
- Replace F with its algebraic closure, then $\min_{T,F}$ splits.
- Claim: in characteristic zero, every irreducible polynomial is separable
  - Proof: it must be the case that either $\gcd(f, f') = 1$ or $f' \equiv 0$, where the second case only happens in characteristic $p > 0$.
  - The first case is true because $\deg f' < \deg f$, and if $\gcd(f, f') = p$, then $\deg p < \deg f$ and $p \mid f$ forces $p = 1$ since f is irreducible.
- So $\min_{T,F}$ splits into distinct linear factors
- Thus T is diagonalizable.

■

11.13 Fall 2020 #8

Let $A \in \operatorname{Mat}(n \times n, \mathbb{C})$ such that the group generated by A under multiplication is finite. Show that

$$\operatorname{Tr}(A^{-1}) = \overline{\operatorname{Tr}(A)},$$

where $\overline{(-)}$ denotes taking the complex conjugate and $\operatorname{Tr}(-)$ is the trace.

12 | Linear Algebra: Canonical Forms

12.1 ⋆ Spring 2012 #8 🚩

Let V be a finite-dimensional vector space over a field k and $T : V \to V$ a linear transformation.

a. Provide a definition for the *minimal polynomial* in $k[x]$ for T.

b. Define the *characteristic polynomial* for T.

c. Prove the Cayley-Hamilton theorem: the linear transformation T satisfies its characteristic polynomial.

12.2 ⋆ Spring 2020 #8 🚩

Let $T : V \to V$ be a linear transformation where V is a finite-dimensional vector space over $\mathbb{C}$. Prove the Cayley-Hamilton theorem: if $p(x)$ is the characteristic polynomial of T, then $p(T) = 0$. You may use canonical forms.

12.3 ⋆ Spring 2012 #7 🚩

Consider the following matrix as a linear transformation from $V := \mathbb{C}^5$ to itself:

$$A = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 \\ -4 & 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

a. Find the invariant factors of A.

b. Express V in terms of a direct sum of indecomposable $\mathbb{C}[x]$-modules.

c. Find the Jordan canonical form of A.

12.4 Fall 2019 Final #8

Exhibit the rational canonical form for

- $A \in M_6(\mathbb{Q})$ with minimal polynomial $(x-1)(x^2+1)^2$.
- $A \in M_{10}(\mathbb{Q})$ with minimal polynomial $(x^2+1)^2(x^3+1)$.

12.5 Fall 2019 Final #9

Exhibit the rational and Jordan canonical forms for the following matrix $A \in M_4(\mathbb{C})$:

$$A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ -2 & -2 & 0 & 1 \\ -2 & 0 & -1 & -2 \end{pmatrix}.$$

12.6 Spring 2016 #7

Let $D = \mathbb{Q}[x]$ and let M be a $\mathbb{Q}[x]$-module such that

$$M \cong \frac{\mathbb{Q}[x]}{(x-1)^3} \oplus \frac{\mathbb{Q}[x]}{(x^2+1)^3} \oplus \frac{\mathbb{Q}[x]}{(x-1)\left(x^2+1\right)^5} \oplus \frac{\mathbb{Q}[x]}{(x+2)\left(x^2+1\right)^2}.$$

Determine the elementary divisors and invariant factors of M.

12.7 Spring 2020 #7

Let

$$A = \begin{bmatrix} 2 & 0 & 0 \\ 4 & 6 & 1 \\ -16 & -16 & -2 \end{bmatrix} \in M_3(\mathrm{C}).$$

a. Find the Jordan canonical form J of A.

b. Find an invertible matrix P such that $P^{-1}AP = J$.

c. Write down the minimal polynomial of A.

You should not need to compute P^{-1}.

12.8 Spring 2019 #7 ✨

Let p be a prime number. Let A be a $p \times p$ matrix over a field F with 1 in all entries except 0 on the main diagonal.

Determine the Jordan canonical form (JCF) of A

a. When $F = \mathbb{Q}$,

b. When $F = \mathbb{F}_p$.

Hint: In both cases, all eigenvalues lie in the ground field. In each case find a matrix P such that $P^{-1}AP$ is in JCF.

Strategy:

- Work with matrix of all ones instead.
- Eyeball eigenvectors.
- Coefficients in minimal polynomial: size of largest Jordan block
- Dimension of eigenspace: number of Jordan blocks
- We can always read off the *characteristic* polynomial from the spectrum.

Concepts Used:

- Todo

Solution:
Proof of (a): Let A be the matrix in the question, and B be the matrix containing 1's in every entry.

- Noting that $B = A + I$, we have

$$\begin{aligned} &B\mathbf{x} = \lambda\mathbf{x} \\ \iff &(A+I)\mathbf{x} = \lambda\mathbf{x} \\ \iff &A\mathbf{x} = (\lambda - 1)\mathbf{x}, \end{aligned}$$

  so we will find the eigenvalues of B and subtract one from each.

- Note that $B\mathbf{v} = \left[\sum v_i, \sum v_i, \cdots, \sum v_i\right]$, i.e. it has the effect of summing all of the entries of $\mathbf{v}$ and placing that sum in each component.

- We proceed by finding p eigenvectors and eigenvalues, since the JCF and minimal polynomials will involve eigenvalues and the transformation matrix will involve (generalized) eigenvectors.

Claim 1: Each vector of the form $\mathbf{p}_i \coloneqq \mathbf{e}_1 - \mathbf{e}_{i+1} = [1, 0, 0, \cdots, 0 - 1, 0, \cdots, 0]$ where $i \neq j$ is also an eigenvector with eigenvalues $\lambda_0 = 0$, and this gives $p - 1$ linearly independent vectors spanning the eigenspace E_{λ_0}

Claim 2: $\mathbf{v}_1 = [1, 1, \cdots, 1]$ is an eigenvector with eigenvalue $\lambda_1 = p$.

- Using that the eigenvalues of A are $1 + \lambda_i$ for λ_i the above eigenvalues for B,

$$\begin{aligned} \operatorname{Spec}(B) \coloneqq \{(\lambda_i, m_i)\} = \{(p, 1), (0, p-1)\} &\implies \chi_B(x) = (x-p)x^{p-1} \\ \implies \operatorname{Spec}(A) = \{(p-1, 1), (-1, p-1)\} &\implies \chi_A(x) = (x - p + 1)(x+1)^{p-1} \end{aligned}$$

- The dimensions of eigenspaces are preserved, thus

$$JCF_{\mathbb{Q}}(A) = J_{p-1}^1 \oplus (p-1) J_{-1}^1 = \left[\begin{array}{r|r|r|c|r|r} p-1 & 0 & 0 & \cdots & 0 & 0 \\ \hline 0 & -1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \ddots & \ddots & 0 \\ \hline 0 & 0 & 0 & \cdots & -1 & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 & -1 \end{array}\right].$$

- The matrix P such that $A = PJP^{-1}$ will have columns the bases of the generalized eigenspaces.

- In this case, the generalized eigenspaces are the usual eigenspaces, so

$$P = [\mathbf{v}_1, \mathbf{p}_1, \cdots, \mathbf{p}_{p-1}] = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 1 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}.$$

Proof (of claim 1).

- Compute

$$B\mathbf{p}_i = [1 + 0 + \cdots + 0 + (-1) + 0 + \cdots + 0] = [0, 0, \cdots, 0]$$

- So every $\mathbf{p}_i \in \ker(B)$, so they are eigenvectors with eigenvalue 0.
- Since the first component is fixed and we have $p - 1$ choices for where to place a -1, this yields $p - 1$ possibilities for $\mathbf{p}_i$
- These are linearly independent since the $(p - 1) \times (p - 1)$ matrix $\left[\mathbf{p}_1^t, \cdots, \mathbf{p}_{p-1}^t\right]$ satisfies

$$\begin{aligned}
\det \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ -1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{bmatrix} &= (1) \cdot \det \begin{bmatrix} -1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{bmatrix} \\
&= (-1)^{p-2} \neq 0.
\end{aligned}$$

where the first equality follows from expanding along the first row and noting this is the first minor, and every other minor contains a row of zeros.

■

Proof (of claim 2).

- Compute

$$B\mathbf{v} = \left[\sum_{i=1}^{p} 1, \sum_{i=1}^{p} 1, \cdots, \sum_{i=1}^{p} 1\right] = [p, p, \cdots, p] = p[1, 1, \cdots, 1] = p\mathbf{v}_1,$$

  thus $\lambda_1 = p$
- $\dim E_{\lambda_1} = 1$ since the eigenspaces are orthogonal and $E_{\lambda_0} \oplus E_{\lambda_1} \leq F^p$ is a subspace, so $p > \dim(E_{\lambda_0}) + \dim E_{\lambda_1} = p - 1 + \dim E_{\lambda_1}$ and it isn't zero dimensional.

■

Proof of (b):
For $F = \mathbb{F}_p$, all eigenvalues/vectors still lie in $\mathbb{F}_p$, but now $-1 = p-1$, making $(x-(p-1))(x+1)^{p-1} = (x+1)(x+1)^{p-1}$, so $\chi_{A,\mathbb{F}_p}(x) = (x+1)^p$, and the Jordan blocks may merge.

- A computation shows that $(A+I)^2 = pA = 0 \in M_p(\mathbb{F}_p)$ and $(A+I) \neq 0$, so $\underset{A,\mathbb{F}_p}{\min}(x) = (x+1)^2$.
  - Thus the largest Jordan block corresponding to $\lambda = -1$ is of size 2
- Can check that $\det(A) = \pm 1 \in \mathbb{F}_p^{\times}$, so the vectors $\mathbf{e}_1 - \mathbf{e}_i$ are still linearly independent and thus $\dim E_{-1} = p - 1$

- So there are $p-1$ Jordan blocks for $\lambda = 0$.

Summary:

$$\begin{aligned}\min_{A,\mathbb{F}_p}(x) &= (x+1)^2 \\ \chi_{A,\mathbb{F}_p}(x) &\equiv (x+1)^p \\ \dim E_{-1} &= p-1.\end{aligned}$$

Thus

$$JCF_{\mathbb{F}_p}(A) = J_{-1}^2 \oplus (p-2)J_{-1}^1 = \left[\begin{array}{cc|c|c|c|c} -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \ddots & \ddots & 0 \\ \hline 0 & 0 & 0 & \cdots & -1 & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 & -1 \end{array}\right].$$

To obtain a basis for $E_{\lambda=0}$, first note that the matrix $P = [\mathbf{v}_1, \mathbf{p}_1, \cdots, \mathbf{p}_{p-1}]$ from part (a) is singular over $\mathbb{F}_p$, since

$$\begin{aligned}\mathbf{v}_1 + \mathbf{p}_1 + \mathbf{p}_2 + \cdots + \mathbf{p}_{p-2} &= [p-1, 0, 0, \cdots, 0, 1] \\ &= [-1, 0, 0, \cdots, 0, 1] \\ &= -\mathbf{p}_{p-1}.\end{aligned}$$

We still have a linearly independent set given by the first $p-1$ columns of P, so we can extend this to a basis by finding one linearly independent generalized eigenvector.
Solving $(A - I\lambda)\mathbf{x} = \mathbf{v}_1$ is our only option (the others won't yield solutions). This amounts to solving $B\mathbf{x} = \mathbf{v}_1$, which imposes the condition $\sum x_i = 1$, so we can choose $\mathbf{x} = [1, 0, \cdots, 0]$. Thus

$$P = [\mathbf{v}_1, \mathbf{x}, \mathbf{p}_1, \cdots, \mathbf{p}_{p-2}] = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 1 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

12.9 Spring 2018 #4

Let

$$A = \begin{bmatrix} 0 & 1 & -2 \\ 1 & 1 & -3 \\ 1 & 2 & -4 \end{bmatrix} \in M_3(\mathbb{C})$$

a. Find the Jordan canonical form J of A.

b. Find an invertible matrix P such that $P^{-1}AP = J$.

You should not need to compute P^{-1}.

12.10 Spring 2017 #6

Let A be an $n \times n$ matrix with all entries equal to 0 except for the $n-1$ entries just above the diagonal being equal to 2.

a. What is the Jordan canonical form of A, viewed as a matrix in $M_n(\mathbb{C})$?

b. Find a nonzero matrix $P \in M_n(\mathbb{C})$ such that $P^{-1}AP$ is in Jordan canonical form.

12.11 Spring 2016 #1

Let

$$A = \begin{pmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{pmatrix} \in M_3(\mathbb{C}).$$

a. Find the Jordan canonical form J of A.

b. Find an invertible matrix P such that $P^{-1}AP = J$. You do not need to compute P^{-1}.

12.12 Spring 2015 #6

Let F be a field and n a positive integer, and consider

$$A = \begin{bmatrix} 1 & \dots & 1 \\ & \ddots & \\ 1 & \dots & 1 \end{bmatrix} \in M_n(F).$$

Show that A has a Jordan normal form over F and find it.

Hint: treat the cases $n \cdot 1 \neq 0$ in F and $n \cdot 1 = 0$ in F separately.

12.13 Fall 2014 #5 🚩

Let T be a 5×5 complex matrix with characteristic polynomial $\chi(x) = (x-3)^5$ and minimal polynomial $m(x) = (x-3)^2$. Determine all possible Jordan forms of T.

12.14 Spring 2013 #5 🚩

Let $T : V \to V$ be a linear map from a 5-dimensional $\mathbb{C}$-vector space to itself and suppose $f(T) = 0$ where $f(x) = x^2 + 2x + 1$.

a. Show that there does not exist any vector $v \in V$ such that $Tv = v$, but there *does* exist a vector $w \in V$ such that $T^2 w = w$.

b. Give all of the possible Jordan canonical forms of T.

12.15 Spring 2021 #1 ✨

Let m

$$A := \begin{bmatrix} 4 & 1 & -1 \\ -6 & -1 & 2 \\ 2 & 1 & 1 \end{bmatrix} \in \operatorname{Mat}(3 \times 3, \mathbb{C}).$$

a. Find the Jordan canonical form J of A.

b. Find an invertible matrix P such that $J = P^{-1}AP$.

c. Write down the minimal polynomial of A.

You should not need to compute P^{-1}

Concepts Used:

- $\chi_A(t) = t^n - \operatorname{tr}\left(\bigwedge^1 A\right) t^{n-1} + \operatorname{tr}\left(\bigwedge^2 A\right) t^{n-2} - \cdots \pm \det(A)$
- Finding generalized eigenvectors: let $B = A - \lambda I$, get eigenvector v, solve $Bw_1 = v, Bw_2 = w_1, \cdots$ to get a Jordan block. Repeat with any other usual eigenvectors.
- Convention: construct Jordan blocks in decreasing order of magnitude of eigenvalues.
- Polynomial exponent data:
  - Minimal polynomial exponents: sizes of **largest** Jordan blocks.

- Characteristic polynomial exponents: **sum of sizes** of Jordan blocks, i.e. how many times λ is on the diagonal of $\mathrm{JCF}(A)$.

Solution:

Proof (parts a and b).

- Write $\chi_A(t) = t^3 - T_1 t^2 + T_2 t - T_3$ where $T_i := \operatorname{tr}\left(\bigwedge^i A\right)$:
  - $T_1 = \operatorname{tr}(A) = 4 - 1 + 1 = 4$.
  - $T_2 = (-1-2) + (4+2) + (-4-6) = 5$.
  - $T_3 = \det(A) = 4(-1-2) - 1(-10) + (-1)(-6+2) = 2$.
- So $\chi_A(t) = t^3 - 4t^2 + 5t - 2$.
- Try rational roots test: $r \in \{\pm 2/1\}$, and check that 2 is root.
- By polynomial long division, $\chi_A(t)/(t-2) = t^2 - 2t + 1 = (t-1)^2$.
- So the eigenvalues are $\lambda = 2, 1$.
- $\lambda = 2$:
  - Set $U := A - \lambda I$, then find $\operatorname{RREF}(U)$ to compute its kernel:

$$U := \begin{bmatrix} 2 & 1 & -1 \\ -6 & -3 & 2 \\ 2 & 1 & -1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

    which yields $v_1 = [1, -2, 0]$.
- $\lambda = 2$:
  - Similarly,

$$U := \begin{bmatrix} 3 & 1 & -1 \\ -6 & -2 & 2 \\ 2 & 1 & 0 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{bmatrix},$$

    which yields $v_2 = [1, -2, 1]$.
  - Solve $Uw = v_3$:

$$\begin{bmatrix} 3 & 1 & -1 & 1 \\ -6 & -2 & 2 & -2 \\ 2 & 1 & 0 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

    so take $v_3 = [0, 1, 0]$.
- Putting things together:

$$A = P^{-1} J P \text{ where}$$

$$J = J_1(\lambda = 2) \oplus J_2(\lambda = 1) = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$P = [v_1, v_2, v_3] = \begin{bmatrix} 1 & 1 & 0 \\ -2 & -2 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

■

Proof (part c).

- Write $\underset{A}{\min}(t) = (t-2)(t-1)^{\ell_1}$, then since $\underset{A}{\min}(t)$ divides $\chi_A(t)$ either $\ell_1 = 1, 2$.
- ℓ_1 is the size of the **largest** block corresponding to $\lambda = 1$, which is size 2, so $\lambda_1 = 2$.
- Thus

$$\underset{A}{\min}(t) = (t-2)(t-1)^2.$$

■

12.16 Fall 2020 #5

Consider the following matrix:

$$B := \begin{bmatrix} 1 & 3 & 3 \\ 2 & 2 & 3 \\ -1 & -2 & -2 \end{bmatrix}.$$

a. Find the minimal polynomial of B.

b. Find a 3×3 matrix J in Jordan canonical form such that $B = JPJ^{-1}$ where P is an invertible matrix.

13 Extra Problems

Many many fundamental problems here: https://math.ucr.edu/~mpierce/teaching/qual-algebra/fun/groups/

13.1 Linear Algebra

1. For a division ring D, let V_i be a finite dimensional vector space over D for $i \in \{1, \ldots, k\}$. Suppose the sequence

$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow \cdots V_k \longrightarrow 0$$

is exact. Prove that $\sum_{i=1}^{k} (-1)^i \dim_D V_i = 0$.

2. Prove that if A and B are invertible matrices over a field $\boldsymbol{k}$, then $A+\lambda B$ is invertible for all but finitely many $\lambda \in \boldsymbol{k}$.
3. For the ring of $n \times n$ matrices over a commutative unital ring R, which we'll denote $\mathrm{Mat}_n(R)$, recall the definition of the determinant map det: $\mathrm{Mat}_n(R) \rightarrow R$. For $A \in \mathrm{Mat}_n(R)$ also recall the definition of the classical adjoint A^a of A. Prove that:

- $\det\left(A^a\right)=\det(A)^{n-1}$
- $\left(A^a\right)^a=\det(A)^{n-2} A$

4. If R is an integral domain and A is an $n \times n$ matrix over R, prove that if a system of linear equations $A x=0$ has a nonzero solution then $\det A=0$. Is the converse true? What if we drop the assumption that R is an integral domain?
5. What is the companion matrix M of the polynomial $f=x^2-x+2$ over C ? Prove that f is the minimal polynomial of M.
6. Suppose that φ and ψ are commuting endomorphisms of a finite dimensional vector space E over a field $\boldsymbol{k}$, so $\varphi \psi=\psi \varphi$.

- Prove that if k is algebraically closed, then φ and ψ have a common eigenvector.
- Prove that if E has a basis consisting of eigenvectors of φ and E has a basis consisting of eigenvectors of ψ, then E has a basis consisting of vectors that are eigenvectors for both φ and ψ simultaneously.

13.2 Galois Theory

Taken from here: https://math.ucr.edu/~mpierce/teaching/qual-algebra/fun/galois/

1. Suppose that for an extension field F over K and for $a \in F$, we have that $b \in F$ is algebraic over $K(a)$ but transcendental over K. Prove that a is algebraic over $K(b)$.
2. Suppose that for a field F/K that $a \in F$ is algebraic and has odd degree over K. Prove that a^2 is also algebraic and has odd degree over K, and furthermore that $K(a)=K\left(a^2\right)$
3. For a polynomial $f \in K[x]$, prove that if $r \in F$ is a root of f then for any $\sigma \in \mathbf{Aut}_K F, \sigma(r)$ is also a root of f
4. Prove that as extensions of $\boldsymbol{Q}, \boldsymbol{Q}(x)$ is Galois over $\boldsymbol{Q}\left(x^2\right)$ but not over $\boldsymbol{Q}\left(x^3\right)$.
5. If F is over E, and E is over K is F necessarily over K ? Answer this question for each of the words "algebraic," "normal," and "separable" in the blanks.
6. If F is over K, and E is an intermediate extension of F over K, is F necessarily over E? Answer this question for each of the words "algebraic," "normal," and "separable" in the blanks.
7. If F is some (not necessarily Galois) field extension over K such that $[F: K]=6$ and Aut $_K F \simeq S_3$, then F is the splitting field of an irreducible cubic over $K[x]$.
8. Recall the definition of the join of two subgroups $H \vee G$ (or $H+G$). For F a finite dimensional Galois extension over K and let A and B be intermediate extensions. Prove that

a. $\operatorname{Aut}_{AB} F=\operatorname{Aut}_{A} F \cap \operatorname{Aut}_{B} F$
b. $\operatorname{Aut}_{A \cap B} F=\operatorname{Aut}_{A} F \vee \operatorname{Aut}_{B} F$

9. For a field K take $f \in K[x]$ and let $n=\deg f$. Prove that for a splitting field F of f over K that $[F : K] \leq n!$. Furthermore prove that $[F : K]$ divides $n!$.
10. Let F be the splitting field of $f \in K[x]$ over K. Prove that if $g \in K[x]$ is irreducible and has a root in F, then g splits into linear factors over F.
11. Prove that a finite field cannot be algebraically closed.
12. For $u=\sqrt{2+\sqrt{2}}$, What is the Galois group of $\boldsymbol{Q}(u)$ over $\boldsymbol{Q}$? What are the intermediate fields of the extension $\boldsymbol{Q}(u)$ over $\boldsymbol{Q}$?
13. Characterize the splitting field and all intermediate fields of the polynomial $\left(x^{2}-2\right)\left(x^{2}-3\right)\left(x^{2}-5\right)$ over Q. Using this characterization, find a primitive element of the splitting field.
14. Characterize the splitting field and all intermediate fields of the polynomial $x^{4}-3$ over Q
15. Consider the polynomial $f=x^{3}-x+1$ in $\boldsymbol{F}_{3}[x]$. Prove that f is irreducible. Calculate the degree of the splitting field of f over $\boldsymbol{F}_{3}$ and the cardinality of the splitting field of f.
16. Given an example of a finite extension of fields that has infinitely many intermediate fields.
17. Let $u=\sqrt{3+\sqrt{2}}$. Is $\boldsymbol{Q}(u)$ a splitting field of u over $\boldsymbol{Q}$? (MathSE)
18. Prove that the multiplicative group of units of a finite field must be cyclic, and so is generated by a single element.
19. Prove that $\boldsymbol{F}_{p^{n}}$ is the splitting field of $x^{p^{n}}-x$ over $\boldsymbol{F}_{p}$.
20. Prove that for any positive integer n there is an irreducible polynomial of degree n over $\boldsymbol{F}_{p}$
21. Recall the definition of a perfect field. Give an example of an imperfect field, and the prove that every finite field is perfect.
22. For $n>2$ let ζ_{n} denote a primitive n th root of unity over Q. Prove that

$$\left[\boldsymbol{Q}\left(\zeta_{n}+\zeta_{n}^{-1} : \boldsymbol{Q}\right)\right]=\frac{1}{2} \varphi(n)$$

where φ is Euler's totient function.
23. Suppose that a field K with characteristic not equal to 2 contains an primitive n th root of unity for some odd integer n. Prove that K must also contain a primitive $2n$ th root of unity.
24. Prove that the Galois group of the polynomial $x^{n}-1$ over Q is abelian.