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

D. Zack Garza

Table of Contents

Contents

Table of Contents 2

1 Group Theory: General 7
- 1.1 Spring 2020 #2 . . . 7
- 1.2 Spring 2019 #4 . . . 7
- 1.3 Spring 2012 #2 . . . 11
- 1.4 Spring 2017 #1 . . . 11
- 1.5 Fall 2016 #1 . . . 11
- 1.6 Fall 2015 #1 . . . 11
- 1.7 Spring 2015 #1 . . . 12
- 1.8 Fall 2014 #6 . . . 12
- 1.9 Spring 2013 #3 . . . 12
- 1.10 Fall 2019 Midterm #1 . . . 12
- 1.11 Fall 2019 Midterm #4 . . . 12
- 1.12 Fall 2019 Midterm #5 . . . 12
- 1.13 Spring 2021 #2 . . . 13

2 Groups: Sylow Theory 13
- 2.1 Fall 2019 #1 . . . 13
- 2.2 Fall 2019 Midterm #2 . . . 15
- 2.3 Fall 2013 #2 . . . 16
- 2.4 Spring 2014 #2 . . . 16
- 2.5 Fall 2014 #2 . . . 16
- 2.6 Spring 2016 #3 . . . 17
- 2.7 Spring 2017 #2 . . . 17
- 2.8 Fall 2017 #2 . . . 17
- 2.9 Fall 2012 #2 . . . 18
- 2.10 Fall 2018 #1 . . . 18
- 2.11 Fall 2019 #2 . . . 19
- 2.12 Spring 2021 #3 . . . 22
- 2.13 Fall 2020 #1 . . . 22
- 2.14 Fall 2020 #2 . . . 22

3 Groups: Group Actions 22
- 3.1 Fall 2012 #1 . . . 22
- 3.2 Fall 2015 #2 . . . 23
- 3.3 Spring 2016 #5 . . . 23
- 3.4 Fall 2017 #1 . . . 23
- 3.5 Fall 2018 #2 . . . 24

4 Groups: Classification 26
- 4.1 Spring 2020 #1 . . . 26

4.2 Spring 2019 #3 ✨ . . . 26
4.3 Spring 2012 #3 🚩 . . . 27
4.4 Fall 2016 #3 🚩 . . . 27
4.5 Spring 2018 #1 ✨ . . . 27

5 Groups: Simple and Solvable **29**
5.1 ⋆ Fall 2016 #7 🚩 . . . 29
5.2 Spring 2015 #4 🚩 . . . 30
5.3 Spring 2014 #1 🚩 . . . 30
5.4 Fall 2013 #1 🚩 . . . 30
5.5 Spring 2013 #4 🚩 . . . 31
5.6 Fall 2019 Midterm #3 🚩 . . . 31

6 Commutative Algebra **31**
6.1 Spring 2020 #5 ✨ . . . 31
6.2 Fall 2019 #3 🚩 . . . 31
6.3 Fall 2019 #6 ✨ . . . 32
6.4 Spring 2019 #6 ✨ . . . 34
6.5 Fall 2018 #7 ✨ . . . 36
6.6 Spring 2018 #5 🚩 . . . 40
6.7 Spring 2018 #8 🚩 . . . 40
6.8 Fall 2017 #5 🚩 . . . 40
6.9 Fall 2017 #6 🚩 . . . 40
6.10 Spring 2017 #3 🚩 . . . 41
6.11 Spring 2017 #4 🚩 . . . 41
6.12 Spring 2016 #8 🚩 . . . 42
6.13 Fall 2015 #3 🚩 . . . 42
6.14 Fall 2015 #4 🚩 . . . 42
6.15 Spring 2015 #7 🚩 . . . 42
6.16 Fall 2014 #7 🚩 . . . 43
6.17 Fall 2014 #8 🚩 . . . 43
6.18 Spring 2014 #5 🚩 . . . 43
6.19 Spring 2014 #6 🚩 . . . 43
6.20 Fall 2013 #3 🚩 . . . 44
6.21 Fall 2013 #4 🚩 . . . 44
6.22 Spring 2013 #1 🚩 . . . 44
6.23 Spring 2013 #2 🚩 . . . 45
6.24 Spring 2021 #5 🚩 . . . 45
6.25 Spring 2021 #6 . . . 45

7 Fields and Galois Theory **46**
7.1 ⋆ Fall 2016 #5 🚩 . . . 46
7.2 ⋆ Fall 2013 #7 🚩 . . . 46
7.3 Fall 2019 #4 ✨ . . . 46
7.4 Fall 2019 #7 ✨ . . . 48
7.5 Spring 2019 #2 ✨ . . . 50
7.6 Spring 2019 #8 ✨ . . . 51
7.7 Fall 2018 #3 ✨ . . . 53

7.8 Spring 2018 #2 ✨ . . . 54
7.9 Spring 2018 #3 ✨ . . . 57
7.10 Spring 2020 #4 🚩 . . . 58
7.11 Spring 2020 #3 🚩 . . . 59
7.12 Fall 2017 #4 🚩 . . . 59
7.13 Fall 2017 #3 🚩 . . . 59
7.14 Spring 2017 #7 🚩 . . . 59
7.15 Spring 2017 #8 🚩 . . . 60
7.16 Fall 2016 #4 🚩 . . . 60
7.17 Spring 2016 #2 🚩 . . . 60
7.18 Spring 2016 #6 🚩 . . . 61
7.19 Fall 2015 #5 🚩 . . . 61
7.20 Fall 2015 #6 🚩 . . . 61
7.21 Spring 2015 #2 🚩 . . . 61
7.22 Spring 2015 #5 🚩 . . . 62
7.23 Fall 2014 #1 🚩 . . . 62
7.24 Fall 2014 #3 🚩 . . . 62
7.25 Spring 2014 #3 🚩 . . . 62
7.26 Spring 2014 #4 🚩 . . . 63
7.27 Fall 2013 #5 🚩 . . . 63
7.28 Fall 2013 #6 🚩 . . . 63
7.29 Spring 2013 #7 🚩 . . . 64
7.30 Spring 2013 #8 🚩 . . . 64
7.31 Fall 2012 #3 🚩 . . . 64
7.32 Fall 2012 #4 🚩 . . . 65
7.33 Spring 2012 #1 🚩 . . . 65
7.34 Spring 2012 #4 🚩 . . . 65
7.35 Fall 2019 Midterm #6 🚩 . . . 65
7.36 Fall 2019 Midterm #7 🚩 . . . 65
7.37 Fall 2019 Midterm #8 🚩 . . . 66
7.38 Fall 2019 Midterm #9 🚩 . . . 66
7.39 Spring 2021 #4 🚩 . . . 66
7.40 Spring 2021 #7 ✨ . . . 66
7.41 Fall 2020 #3 🚩 . . . 68
7.42 Fall 2020 #4 🚩 . . . 68

8 Modules **69**
8.1 General Questions . . . 69
8.1.1 Fall 2018 #6 ✨ . . . 69
8.1.2 Fall 2019 Final #2 🚩 . . . 70
8.1.3 Spring 2018 #6 🚩 . . . 70
8.1.4 Spring 2018 #7 🚩 . . . 71
8.1.5 Fall 2016 #6 🚩 . . . 71
8.1.6 Spring 2016 #4 🚩 . . . 71
8.1.7 Spring 2015 #8 🚩 . . . 71
8.1.8 Fall 2012 #6 🚩 . . . 72
8.1.9 Fall 2019 Final #1 🚩 . . . 72
8.1.10 Fall 2020 #6 🚩 . . . 72

8.2 Torsion and the Structure Theorem . . . 72
8.2.1 ⋆ Fall 2019 #5 ✨ . . . 72
8.2.2 ⋆ Spring 2019 #5 ✨ . . . 74
8.2.3 ⋆ Spring 2020 #6 ✨ . . . 77
8.2.4 Spring 2012 #5 🚩 . . . 82
8.2.5 Spring 2017 #5 🚩 . . . 82
8.2.6 Fall 2019 Final #3 🚩 . . . 83
8.2.7 Fall 2019 Final #4 🚩 . . . 83
8.2.8 Fall 2019 Final #5 🚩 . . . 83
8.2.9 Fall 2019 Final #6 🚩 . . . 83
8.2.10 Fall 2019 Final #7 🚩 . . . 83
8.2.11 Fall 2019 Final #10 🚩 . . . 83
8.2.12 Fall 2020 #7 🚩 . . . 84

9 Linear Algebra: Diagonalizability 84
9.1 Fall 2017 #7 🚩 . . . 84
9.2 Spring 2015 #3 🚩 . . . 85
9.3 Fall 2016 #2 🚩 . . . 85
9.4 Spring 2019 #1 ✨ . . . 85

10 Linear Algebra: Misc 87
10.1 ⋆ Spring 2012 #6 🚩 . . . 87
10.2 ⋆ Spring 2014 #7 🚩 . . . 87
10.3 Fall 2012 #7 🚩 . . . 87
10.4 Fall 2012 #8 🚩 . . . 88
10.5 Fall 2012 #5 🚩 . . . 88
10.6 Fall 2015 #7 🚩 . . . 88
10.7 Fall 2014 #4 🚩 . . . 88
10.8 Fall 2015 #8 🚩 . . . 89
10.9 Fall 2018 #4 ✨ . . . 89
10.10 Fall 2018 #5 ✨ . . . 90
10.11 Fall 2019 #8 🚩 . . . 92
10.12 Spring 2013 #6 ✨ . . . 94
10.13 Fall 2020 #8 🚩 . . . 96

11 Linear Algebra: Canonical Forms 97
11.1 ⋆ Spring 2012 #8 🚩 . . . 97
11.2 ⋆ Spring 2020 #8 🚩 . . . 97
11.3 ⋆ Spring 2012 #7 🚩 . . . 97
11.4 Fall 2019 Final #8 🚩 . . . 98
11.5 Fall 2019 Final #9 🚩 . . . 98
11.6 Spring 2016 #7 🚩 . . . 98
11.7 Spring 2020 #7 🚩 . . . 98
11.8 Spring 2019 #7 ✨ . . . 99
11.9 Spring 2018 #4 🚩 . . . 103
11.10 Spring 2017 #6 🚩 . . . 103
11.11 Spring 2016 #1 🚩 . . . 103
11.12 Spring 2015 #6 🚩 . . . 104

11.13Fall 2014 #5 104
11.14Spring 2013 #5 104
11.15Spring 2021 #1 104
11.16Fall 2020 #5 105

1 | Group Theory: General

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.

Work this problem.

1.2 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.

Concepts Used:

- Notation: X/G is the set of G-orbits
- Notation: $X^g = \left\{ x \in x \;\middle|\; g \cdot x = x \right\}$
- Burnside's formula: $|G||X/G| = \sum |X^g|$.

Strategy:
Burnside.

Solution:

Proof (Part a).
Strategy: Burnside.

- Define a sample space $\Omega = G \times G$, so $|\Omega| = |G|^2$.
- Identify the event we want to analyze: $A \coloneqq \left\{(g,h) \in G \times G \;\middle|\; [g,h] = 1\right\}$.
  - Define and note:
$$A_g \coloneqq \left\{(g,h) \;\middle|\; h \in H, [g,h] = 1\right\} \implies A = \coprod_{g\in G} A_g.$$
- 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.
  - 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 precisely A_g.
- Note $|X/G| = n$, the number of conjugacy classes.
- Note that
$$|A| = \left|\coprod_{g\in G} A_g\right| = \sum_{g\in G} |A_g| = \sum_{g\in G} |X^g|.$$
- Apply Burnside
$$|X/G| = \frac{1}{|G|}\sum_{g\in G} |X^g|,$$
- Rearrange and use definition:
$$n|G| = |X/G||G| = \sum_{g\in G} |X^g|$$
- Compute probability:
$$P(A) = \frac{|A|}{|\Omega|} = \frac{\sum_{g\in G}|X^g|}{|G|^2} = \frac{|X/G||G|}{|G|^2} = \frac{n|G|}{|G|^2} = \frac{n}{|G|}.$$

■

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 $Z(x) = \left\{ g \in G \;\middle|\; [g, x] = 1 \right\}$.

■

Proof (Part c).
As shown in part 1,

$$\mathcal{O}_x = \left\{ g \curvearrowright x \;\middle|\; g \in G \right\} = \left\{ h \in G \;\middle|\; ghg^{-1} = h \right\} = C_G(g),$$

and by the class equation

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

Now note

- Each element of $Z(G)$ is in its own conjugacy class, contributing $|Z(G)|$ classes to n.
- Every other class of elements in $G \setminus Z(G)$ contains at least 2 elements
  - Claim: each such class contributes **at least** $\frac{1}{2}|G \setminus Z(G)|$.

Thus

$$\begin{aligned} n &\leq |Z(G)| + \frac{1}{2}|G \setminus Z(G)| \\ &= |Z(G)| + \frac{1}{2}|G| - \frac{1}{2}|Z(G)| \\ &= \frac{1}{2}|G| + \frac{1}{2}|Z(G)| \end{aligned}$$

$$\begin{aligned} \implies \frac{n}{|G|} &\leq \frac{1}{2}\frac{|G|}{|G|} + \frac{1}{2}\frac{|Z(G)|}{|G|} \\ &= \frac{1}{2} + \frac{1}{2}\frac{1}{[G : Z(G)]}. \end{aligned}$$

■

Redo part c

1.3 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.

1.4 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.

1.5 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

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

1.6 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.

1.7 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.

1.8 Fall 2014 #6

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

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

1.9 Spring 2013 #3

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

1.10 Fall 2019 Midterm #1

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

1.11 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.

1.12 Fall 2019 Midterm #5

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

1.13 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.

2 | Groups: Sylow Theory

2.1 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:

- Centralizer:

$$C_G(h) = Z(h) = \left\{ g \in G \;\middle|\; [g,h] = 1 \right\} \quad \text{Centralizer}$$

- Class equation:

$$|G| = \sum_{\substack{\text{One } h \text{ from each} \\ \text{conjugacy class}}} \frac{|G|}{|Z(h)|}$$

- Notation:

$$\begin{aligned} h^g &= ghg^{-1} \\ h^G &= \left\{ h^g \;\middle|\; g \in G \right\} \quad \text{Conjugacy Class} \\ H^g &= \left\{ h^g \;\middle|\; h \in H \right\} \\ N_G(H) &= \left\{ g \in G \;\middle|\; H^g = H \right\} \supseteq H \quad \text{Normalizer.} \end{aligned}$$

Solution:

Claim 1:

$$\left| h^G \right| = [G : Z(h)].$$

Claim 2:

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

Proof (of claim 2).

- Let $G \curvearrowright \left\{H \;\middle|\; H \leq G\right\}$ by $H \mapsto gHg^{-1}$.
- Then the $\mathcal{O}_H$ is the set of conjugate subgroups, $\text{Stab}(H) = N_G(H)$.
- So Orbit-Stabilizer says $\mathcal{O}_h \cong G/\text{Stab}(H)$; then just take sizes.

■

Claim 3: $\cup_{g\in G} H^g = \cup_{g\in G} gHg^{-1} \subsetneq G$ for any proper $H \leq G$.

Proof (of claim 3).

- By theorem 2, since each coset is of size $|H|$, which only intersect at the identity, and there are exactly $[G : N_G(H)]$ of them

$$\begin{aligned}
|\cup_{g\in G} H^g| &= (|H| - 1)\,[G : N_G(H)] + 1 \\
&= |H|[G : N_G(H)] - [G : N_G(H)] + 1 \\
&= |G|\frac{|G|}{|N_G(H)|} - \frac{|G|}{|N_G(H)|} + 1 \\
&\leq |H|\frac{|G|}{|H|} - \frac{|G|}{|H|} + 1 \\
&= |G| - ([G : H] - 1) \\
&< |G|,
\end{aligned}$$

  where we use the fact that $H \subseteq N_G(H) \implies |H| \leq |N_G(H)| \implies \dfrac{1}{|N_G(H)|} \leq \dfrac{1}{|H|}$, and since $H < G$ is proper, $[G : H] \geq 2$.

- Since $[g_i, g_j] = 1$, we have $g_i \in Z(g_j)$ for every i, j.
- Then

$$\begin{aligned}
g \in G &\implies g = g_i^h \quad \text{for some } h \\
&\implies g \in Z(g_{\mathbf{j}})^h \quad \text{for every } j \text{ since } g_i \in Z(g_j)\ \forall j \\
&\implies g \in \cup_{h\in G} Z(g_j)^h \quad \text{for every } j \\
&\implies G \subseteq \cup_{h\in G} Z(g_j)^h \quad \text{for every } j,
\end{aligned}$$

  which by Theorem 3, if $Z(g_j) < G$ were proper, then the RHS is properly contained in G.

- So it must be the case that that $Z(g_j)$ is not proper and thus equal to G for every j.
- But $Z(g_i) = G \iff g_i \in Z(G)$, and so each conjugacy class is size one.
- So for every $g \in G$, we have $g = g_j$ for some j, and thus $g = g_j \in Z(g_j) = Z(G)$, so g is central.
- Then $G \subseteq Z(G)$ and G is abelian.

■

2.2 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.

2.3 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).

2.4 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.

2.5 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.

2.6 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.

2.7 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.

2.8 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.

2.9 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.

2.10 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 $S_p^i \in \mathrm{Syl}_p(G)$.
- $P \trianglelefteq G \iff gPg^{-1} = P$ 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

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

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

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

■

2.11 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 $n_p \cong 1 \pmod{p}$.
- **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, $q - 1 \neq 0 \pmod{p}$.
- **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
- $n_3 \mid 5 \cdot 7, \quad n_3 \cong 1 \pmod{3} \implies n_3 \in \{1, 5, 7, 35\} \setminus \{5, 35\}$
- $n_5 \mid 3 \cdot 7, \quad n_5 \cong 1 \pmod{5} \implies n_5 \in \{1, 3, 7, 21\} \setminus \{3, 7\}$
- $n_7 \mid 3 \cdot 5, \quad n_7 \cong 1 \pmod{7} \implies n_7 \in \{1, 3, 5, 15\} \setminus \{3, 5\}$
- 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

  $|\mathrm{Syl}(5) \cup \mathrm{Syl}(7)| = (5-1)n_5 + (7-1)n_7 + 1 = 4(21) + 6(15) = 174 > 105$ 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** ($n_5 = 21$ or $n_7 = 15$), which is equivalent to ($n_5 = 1$ 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 ≥ 31.
  - Elements in G of order **not** equal to 7 ≥ 29.
- Now both cases lead to contradictions:
  - $n_5 = 21$:

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

  - $n_7 = 15$:

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

■

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.

■

2.12 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.

2.13 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.

2.14 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.

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 and let $y\in G_x$ be another element in the orbit of x.
- Then there exists a $g\in G$ such that $g\cdot x = y$, so $x = g^{-1}\cdot y$
- Then

$$\begin{aligned}
h\in G\cdot x &\iff h\cdot x = x && \text{by being in the stabilizer}\\
&\iff h\cdot(g^{-1}\cdot y) = g^{-1}\cdot y && \text{using that } x,y \text{ are in the same orbit}\\
&\iff (ghg^{-1})\cdot y = y\\
&\iff ghg^{-1}\in G_y && \text{by the defn of the stabilizer}\\
&\iff h\in g^{-1}G_y g,
\end{aligned}$$

so every $h\in G\cdot x$ is conjugate to some element in G_y.

■

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

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

- Note that $X^e = X$, since the identity must fix every element, so $|X^e| \geq 2$.
- Not *every* other term in the sum can be greater than 1, otherwise the RHS is greater than the size of G
- Thus we must have $|X^g| = 0$ for some $g \in G$, i.e. g has no fixed points in X.

■

4 | Groups: Classification

4.1 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.

4.2 Spring 2019 #3

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

Describe a representative from each class.

Concepts Used:

- Sylow theorems:
- $n_p \cong 1 \pmod p$

- $n_p \mid m$.

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.

4.3 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.

4.4 Fall 2016 #3

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

4.5 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

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

  - 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
  - $n_5 \mid 7^2, \quad n_5 \cong 1 \pmod 5 \implies n_5 \in \{1, 7, 49\} \setminus \{7, 49\} = \{1\} \implies n_5 = 1$
  - $n_7 \mid 5^2, \quad n_7 \cong 1 \pmod 7 \implies n_7 \in \{1, 5, 25\} \setminus \{5, 25\} = \{1\} \implies n_7 = 1$
- 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).

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

■

5 | Groups: Simple and Solvable

5.1 ⋆ 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.

5.2 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 $n \equiv 2 \pmod 4$. Prove that G is not simple.

Hint: use part (b).

5.3 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.

5.4 Fall 2013 #1

Let p, q be distinct primes.

a. Let $\bar{q} \in \mathbb{Z}_p$ be the class of $q \pmod p$ 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.

5.5 Spring 2013 #4

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

5.6 Fall 2019 Midterm #3

Show that there exist no simple groups of order 148.

6 Commutative Algebra

6.1 Spring 2020 #5

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

6.2 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.

Concepts Used:

- Todo

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).

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

■

6.3 Fall 2019 #6 ✨

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

a. Show that

$$N = \{r \in R \mid r^n = 0 \text{ for some } n > 0\}$$

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.

■

6.4 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 $J \coloneqq \cup J_i$, 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, $\impliedby$).
$\impliedby$

- 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

$$M' \coloneqq \left\{ rx + m \;\middle|\; r \in R,\ m \in M \right\}.$$

- 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). • We want to show $J(R) = \mathfrak{N}(R)$.
$\mathfrak{N}(R) \subseteq J(R)$:

- We'll 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

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

■

6.5 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:

- Todo
- 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).

- We identify $\ker\varphi = \left\{x \in R \;\middle|\; rx = 0\right\}$, and since $r \neq 0$ by assumption, this implies each such x is a zero divisor by definition (and $\ker\varphi$ is nonempty by assumption).
- Similarly, we identify $\operatorname{im}\varphi = \left\{y = rx \;\middle|\; x \in R\right\}$. So let $y \in \operatorname{im}\varphi$.
- Since r is a zero divisor, there exists some $z \in R$ such that $rz = 0$.
- But then

$$yz = rxz = xrz = x \cdot 0 = 0$$

since R is commutative, so y is a zero divisor.

■

Proof (of c).

- Let $Z \coloneqq \{z_i\}_{i=1}^n$ 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 $R/K_i \coloneqq \{r + K_i\}$.
- 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

$$\left[\begin{array}{c|cc} & t & 1+t \\ \hline t & 1+t & 1 \\ t & 1 & t \end{array}\right],$$

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

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

■

6.6 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

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

6.7 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 $Z(I) = \{x \in [0,1] \;\middle|\; f(x) = 0 \text{ for all } f \in I\}$ is nonempty.

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

6.8 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.

6.9 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.

6.10 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.

6.11 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 $p(x) = x^2 - 2$.

6.12 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.

6.13 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.

6.14 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 $j \geq n$.

6.15 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.

6.16 Fall 2014 #7

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

6.17 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.

6.18 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 $a^n = 0$.

6.19 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.

6.20 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.

6.21 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.

6.22 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

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

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 $I = \mathrm{Ann}(\mu)$ for some $\mu \in M$. In other words, $I = \mathrm{Ann}(\mu)$ but there does not exist $\nu \in M$ with $J = \mathrm{Ann}(\nu) \subsetneq R$ such that $I \subsetneq J$.

Prove that I is a prime ideal.

6.23 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.

6.24 Spring 2021 #5

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 $af(x) = 0$.

6.25 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 $\left\{ 2x^k \;\middle|\; 1 \leq k \in \mathbb{Z} \right\}$.

7 | Fields and Galois Theory

7.1 ⋆ Fall 2016 #5

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

7.2 ⋆ 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.

7.3 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 $\left|E^\times\right| = q^k - 1$.
- Noting that $\zeta \in E^\times$ we must have $n = o(\zeta) \mid \left|E^\times\right| = q^k - 1$ by Lagrange's theorem.

■

Proof (of b).

- Rephrasing (a), we have

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

■

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 $k = m$.

■

7.4 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:

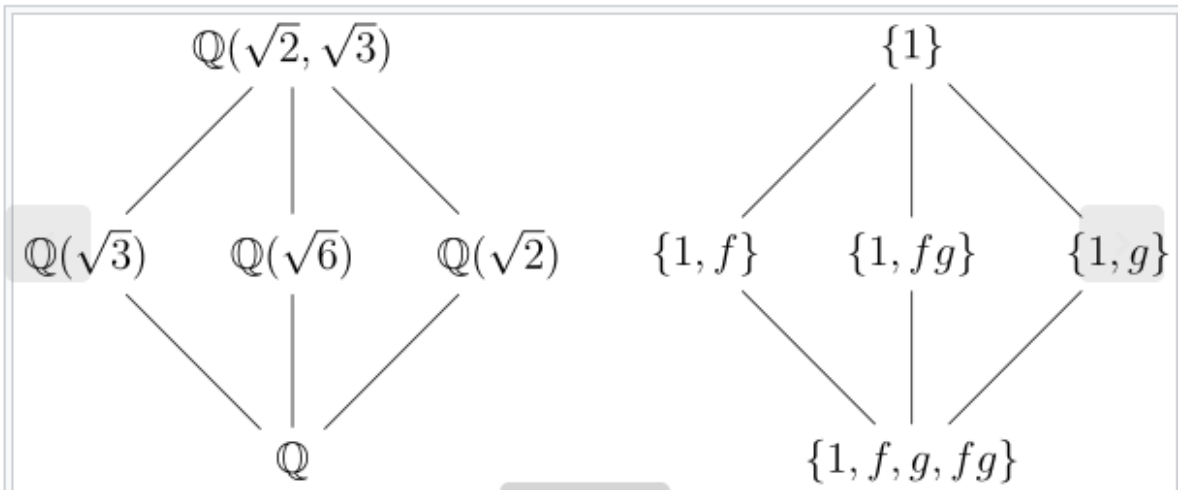


Figure 1: image_2021-04-17-02-44-48

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 $f(x) = \prod_{k \le n} (x - \zeta^k)$.

Since it is a Galois extension, $|\text{Gal}(K/\mathbb{Q})| = [K:\mathbb{Q}] = \varphi(n)$ 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 $\text{Gal}(K/\mathbb{Q})$.
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.

■

7.5 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 $\varphi_n(x) \coloneqq x^{p^n} - x$; 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.

■

■

7.6 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:

- $\zeta_n \coloneqq e^{\frac{2\pi i}{n}}$, 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

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

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

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).

- $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/(8)^\times \cong \mathbb{Z}/(4)$ 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 $\zeta_8 + \zeta_8^{-1} = 2/\sqrt{2} = \sqrt{2}$.
  - $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(i, \sqrt{2})$:
    - ♢ $\zeta = e^{2\pi i/8} = \sin(\pi/4) + i\cos(\pi/4) = \dfrac{\sqrt{2}}{2}(1+i)$.
- 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.

■

7.7 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 $f(x) \coloneqq \min(\alpha, F)$ has no repeated factors, then $f'(x) \coloneqq \min(\alpha, K)$ 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.)
■

7.8 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.

Concepts Used:

- Todo

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 $L \coloneqq \mathbb{Q}(\sqrt{2})$, 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 $|\mathrm{Gal}(K/\mathbb{Q})| = 4$, which leaves only two possibilities:

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

We can next check orders of elements. Take

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

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

■

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)

7.9 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 $E = E_1E_2 \subset K$.

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

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

b. Show that H_1H_2 is a subgroup of G.

c. Show that

$$\text{Gal}(K/(E_1 \cap E_2)) = H_1H_2.$$

Concepts Used:

- The Galois correspondence:
  - $H_1 \cap H_2 \rightleftharpoons E_1E_2$,
  - $H_1H_2 \rightleftharpoons E_1 \cap E_2$.

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 $\sigma \in \text{Aut}(K)$ 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 $H_1H_2 \leq G$ will correspond to an intermediate field E such that $K/E/\mathbb{Q}$ and E is the fixed field of H_1H_2.
But if $\sigma \in H_1H_2$, then $\sigma = \tau_1\tau_2$ where τ_i is an automorphism of K that fixes E_i, and so

$$\sigma(x) = x \iff \tau_1\tau_2(x) = x \iff \tau_2(x) = x$$
$$\&$$
$$\tau_1(x) = x \iff x \in E_1 \cap E_2.$$

.

■

7.10 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 $\mathrm{Gal}(E/\mathbb{Q})$ 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.

7.11 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.

7.12 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 $\mathbb{Q}$.

7.13 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.

7.14 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.

7.15 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 $\mathbb{Q}$.

7.16 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.

7.17 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.

7.18 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.

7.19 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 $\mathbb{Q} \subset F \subset E$.

7.20 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.

7.21 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.

7.22 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 $\mathbb{Q}(\sqrt{5})$.

7.23 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.

7.24 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.

7.25 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.

7.26 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.

7.27 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.

7.28 Fall 2013 #6

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

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 $N = \text{Gal}(K/\mathbb{Q}(i))$ and $H = \text{Gal}(K/\mathbb{Q}(\sqrt[4]{2}))$. 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.

7.29 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 $\alpha = \sqrt{2} + \sqrt{3}$.

7.30 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 $\beta \in K$.

7.31 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.

7.32 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.

7.33 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.

7.34 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 $E \neq \mathbb{Q}(\alpha)$.

7.35 Fall 2019 Midterm #6

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

7.36 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 $y^p = x$.

7.37 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.

7.38 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. 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 $[L : K]$.

7.39 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.

7.40 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:

- 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 $\mathrm{SF}(f)[x]$.
- Bezout's identity: $\gcd(p, q) = d \implies$ there exist $s, t \in \mathbb{Z}$ such that

$$sp + tq = d.$$

Solution:

- WTS: $f(x) \coloneqq x^p - a \in \mathbb{F}[x]$ 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 $R_\ell \coloneqq \prod_{i=1}^{\ell} r_i$, 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?

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

  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.

7.41 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 $\mathbb{Q}$.

7.42 Fall 2020 #4

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

8 | Modules

8.1 General Questions

8.1.1 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 subgroup. 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.

■

8.1.2 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 $\mathbb{Z}^3/N$.

8.1.3 Spring 2018 #6

Let

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

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

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

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

8.1.4 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 $k \geq 0$.

8.1.5 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 $N \cong \operatorname{im} f \oplus \ker g$.

8.1.6 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:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

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

8.1.7 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.

8.1.8 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.

8.1.9 Fall 2019 Final #1

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

8.1.10 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

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

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.

8.2 Torsion and the Structure Theorem

8.2.1 ⋆ 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

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

We have

$$\begin{aligned} t_1 \in \mathrm{Tor}(M) &\implies \exists s_1 \neq 0 \text{ such that } s_1 t_1 = 0 \\ t_2 \in \mathrm{Tor}(M) &\implies \exists s_2 \neq 0 \text{ such that } s_2 t_2 = 0. \end{aligned}$$

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 $b \curvearrowright m \coloneqq bm \in M$ as well, but then

$$a \curvearrowright bm = (ab) \curvearrowright m = 0 \curvearrowright m = 0_M,$$

so m is a torsion element for any m.

■

8.2.2 ⋆ 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 $\tilde{M} \coloneqq M/\operatorname{Tor}(M)$ and $\pi : M \to M'$ be the canonical quotient map.

Claim:

$$\tilde{\mathcal{B}} \coloneqq \pi(\mathcal{B}) = \{\mathbf{r}_i + \operatorname{Tor}(M)\}$$

is a basis for $\tilde{M}$.
Note that the proof follows immediately.

■

Proof (of claim: linearly independent).

- Suppose that

$$\sum_{i=1}^{n} s_i(\mathbf{r}_i + \operatorname{Tor}(M)) = \mathbf{0}_{\tilde{M}}.$$

- Then using the definition of coset addition/multiplication, we can write this as

$$\sum_{i=1}^{n} (s_i\mathbf{r}_i + \operatorname{Tor}(M)) = \left(\sum_{i=1}^{n} s_i\mathbf{r}_i\right) + \operatorname{Tor}(M) = 0_{\tilde{M}}.$$

- Since $\tilde{\mathbf{x}} = 0 \in \tilde{M} \iff \tilde{\mathbf{x}} = \mathbf{x} + \operatorname{Tor}(M)$ where $\mathbf{x} \in \operatorname{Tor}(M)$, this forces $\sum s_i\mathbf{r}_i \in \operatorname{Tor}(M)$.
- 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 $\pi(\mathcal{B}) = \{\mathbf{r}_i + \operatorname{Tor}(M)\}_{i=1}^n$ as a set of cosets.
- Letting $\mathbf{x} \in M'$ be arbitrary, we can write $\mathbf{x} = \mathbf{m} + \operatorname{Tor}(M)$ 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

$$\begin{aligned}
\mathbf{x} &= \pi(\mathbf{m}) \\
&\coloneqq \pi\left(\sum_{i=1}^{n} s_i\mathbf{r}_i\right) \\
&= \sum_{i=1}^{n} s_i\pi(\mathbf{r}_i) \quad \text{since } \pi \text{ is an } R\text{-module morphism} \\
&\coloneqq \sum_{i=1}^{n} s_i(\mathbf{r}_i + \operatorname{Tor}(M)),
\end{aligned}$$

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 $\text{rank}_R(M) \geq 1$, 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 $M \subseteq R$, so $\alpha\mathbf{m} = \mathbf{0} \implies \alpha = 0_R$.
- Claim: since R is commutative, $\text{rank}_R(M) \leq 1$.
  - 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 $\mathbf{x} \in \text{Tor}\, M$, 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 $\text{Tor}(M) = \{0_R\}$.

■

■

8.2.3 ⋆ 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:

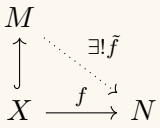
- M admits an R-linearly independent spanning set $\{\mathbf{b}_\alpha\}$, so

$$m \in M \implies m = \sum_\alpha r_\alpha \mathbf{b}_\alpha$$

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:



Equivalently,

$$\underset{\mathsf{Set}}{\mathrm{Hom}}(X, \mathrm{Forget}(N)) \xrightarrow{\sim} \underset{\mathsf{R\text{-}Mod}}{\mathrm{Hom}}(M, N).$$

■

Proof (of b).

- Define the annihilator:

$$\operatorname{Ann}(m) \coloneqq \left\{ r \in R \;\middle|\; r \cdot m = 0_M \right\} \trianglelefteq R.$$

  - Note that $mR \cong R/\operatorname{Ann}(m)$.

- Define the torsion submodule:

$$M_t \coloneqq \left\{ m \in M \;\middle|\; \operatorname{Ann}(m) \neq 0 \right\} \leq M$$

- M is **torsionfree** iff $M_t = 0$ is the trivial submodule.

■

Proof (of c).

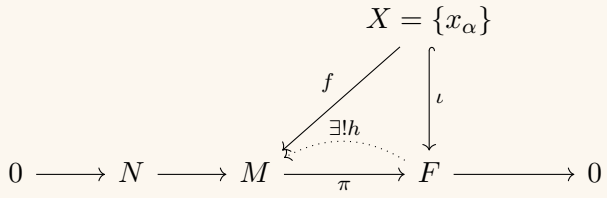
- Let the following be an SES where F is a free R-module:

$$0 \to N \to M \xrightarrow{\pi} F \to 0.$$

- 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 $h : F \to M$:



- 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

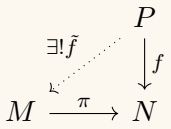
$$\begin{aligned} (\pi \circ h)(f) &= (\pi \circ h)\left(\sum r_i x_i\right) \\ &= \sum r_i (\pi \circ h)(x_i), \end{aligned}$$

  but since $h(x_i) \in \pi^{-1}(x_i)$, we have $(\pi \circ h)(x_i) = x_i$. So this recovers f.

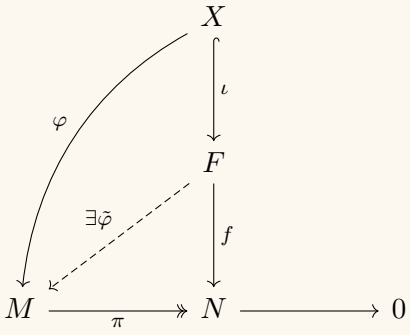
■

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 $\tilde{f} : P \to M$:

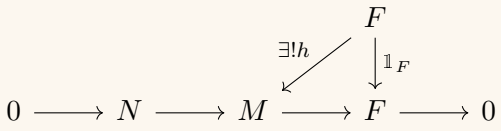


  - Construct φ in the following diagram using the same method as above (surjectivity to pick elements in preimage):



Link to Diagram

- Now take the identity map, then commutativity is equivalent to being a section.



■

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 $M \cong M_t \oplus \dfrac{M}{M_t}$, 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

$$M_t = r(m + M_t) \coloneqq (rm) + M_t \implies rm \in M_t.$$

- 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 $m \in M_t$

■

8.2.4 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.

8.2.5 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.

8.2.6 Fall 2019 Final #3

Let $R = k[x]$ for k a field and let M be the R-module given by

$$M = \frac{k[x]}{(x-1)^3} \oplus \frac{k[x]}{(x^2+1)^2} \oplus \frac{k[x]}{(x-1)(x^2+1)^4} \oplus \frac{k[x]}{(x+2)(x^2+1)^2}.$$

Describe the elementary divisors and invariant factors of M.

8.2.7 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.

8.2.8 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.

8.2.9 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 $S \circ T \neq 0$.

8.2.10 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.

8.2.11 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.

8.2.12 Fall 2020 #7

Let $A \in \mathrm{Mat}(n \times n, \mathbb{R})$ be arbitrary. Make $\mathbb{R}^n$ into an $\mathbb{R}[x]$-module by letting $f(x).\mathbf{v} \coloneqq f(A)(\mathbf{v})$ 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.

9 | Linear Algebra: Diagonalizability

9.1 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.

9.2 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.

9.3 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.

9.4 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

$$q_A(x) \coloneqq \min_{A^n}(x^n) = \prod_{i=1}^{m}(x^n - \lambda_i) \in \mathbb{F}[x],$$

  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 $\bar{\mathbb{F}}[x]$

- 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

$$x^n - \lambda_i = \prod_{k=1}^{n}(x - \lambda_i^{\frac{1}{n}} e^{\frac{2\pi i k}{n}}) \coloneqq \prod_{k=1}^{n}(x - \lambda^{\frac{1}{n}}\zeta_n^k),$$

  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 $\dfrac{\partial}{\partial x}(x^n - \lambda_i) = nx^{n-1} \neq 0 \in \mathbb{F}$, 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 $\bar{\mathbb{F}}[x]$ 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 $\mathbb{F}$. ■

10 | Linear Algebra: Misc

10.1 ⋆ 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.

10.2 ⋆ 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

$$(P,Q) \cdot A \coloneqq PAQ^{-1}$$

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.

10.3 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.

10.4 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.

10.5 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 $W' \cong W$.

10.6 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.

10.7 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.

10.8 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.

10.9 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.

10.10 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, $\implies$).
$\implies$:
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.

■

Proof (of b, $\impliedby$).
$\impliedby$:
Let $A \curvearrowright k[x]$ by $A \curvearrowright p(x) \coloneqq p(A)$. 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 $\operatorname{Ann}(\mathbf{v}) = \chi_A(x)$, 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

$$\begin{aligned}
V &\cong k[x] \curvearrowright \mathbf{v} \\
&\coloneqq \left\{f(x) \curvearrowright \mathbf{v} \;\middle|\; f \in k[x]\right\} \\
&= \operatorname{span}_k \left\{x^k \curvearrowright \mathbf{v} \;\middle|\; k \geq 0\right\} \\
&\coloneqq \operatorname{span}_k \left\{A^k \mathbf{v} \;\middle|\; k \geq 0\right\}.
\end{aligned}$$

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

$$\begin{aligned}
V &\cong \operatorname{span}_k \left\{A^\ell \mathbf{v} \;\middle|\; \ell \geq 0\right\} \\
&= \operatorname{span}_k \left\{A^\ell \mathbf{v} \;\middle|\; 1 \leq \ell \leq n-1\right\}.
\end{aligned}$$

■

10.11 Fall 2019 #8

Let $\{e_1, \cdots, e_n\}$ be a basis of a real vector space V and let

$$\Lambda \coloneqq \left\{ \sum r_i e_i \;\middle|\; r_i \in \mathbb{Z} \right\}$$

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

$$\Lambda^\vee \coloneqq \{v \in V \;|\; v \cdot x \in \mathbb{Z} \text{ for all } x \in \Lambda\}.$$

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.

$$\begin{aligned}
\mathbf{v} \in \Lambda^\vee &\implies \langle \mathbf{e}_i,\ \mathbf{v} \rangle = z_i \in \mathbb{Z} \quad \forall i \\
&\implies A^t \mathbf{v} = \mathbf{z} \coloneqq [z_1, \cdots, z_n] \in \mathbb{Z}^n \\
&\implies \mathbf{v} = A^{-t}\mathbf{z} \coloneqq B\mathbf{z} \in \operatorname{im} B \\
&\implies \mathbf{v} \in \operatorname{im} B \\
&\implies \Lambda^\vee \subseteq \operatorname{im} B,
\end{aligned}$$

and

$$\begin{aligned}
B^t A = (A^{-t})^t A = A^{-1} A = I \\
\implies \mathbf{b}_i \cdot \mathbf{e}_j = \delta_{ij} \in \mathbb{Z} \\
\implies \operatorname{im} B \subseteq \operatorname{span} \Lambda^\vee.
\end{aligned}$$

10.12 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 $\iff$ $\chi_T(x)/\urcorner$ 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 $f \coloneqq \chi_{V,T}(x)$ is reducible.
- Since $T(W) \subseteq W$, the restriction $g \coloneqq \chi_{V,T}(x)\Big|_W : W \to W$ 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 $\mathcal{B}_W \coloneqq \{\mathbf{w}_1, \cdots, \mathbf{w}_k\}$ where $k = \dim_F(W)$
- Claim: this can be extended to a basis of V, say $\mathcal{B}_V \coloneqq \{\mathbf{w}_1, \cdots, \mathbf{w}_k, \mathbf{v}_1, \cdots, \mathbf{v}_j\}$ 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

  $$\chi_{T,V}(x) \coloneqq \det([T]_{\mathcal{B}_V} - xI) = \det(B - xI) \cdot \det(D - xI) \coloneqq \chi_{T,W}(x) \cdot \det(D - xI).$$

- 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 $\min\limits_{T,F}(x)$ be the minimal polynomial of T and $\chi_{T,F}(x)$ be its characteristic polynomial.
- By Cayley-Hamilton, $\min\limits_{T,F}(x)$ divides $\chi_{T,F}$
- Since $\chi_{T,F}$ is irreducible, these polynomials are equal.
- Claim: T/F is diagonalizable $\iff$ $\min\limits_{T,F}$ splits over F and is squarefree.
- Replace F with its algebraic closure, then $\min\limits_{T,F}$ 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 $\min\limits_{T,F}$ splits into distinct linear factors
- Thus T is diagonalizable.

■

10.13 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.

11 | Linear Algebra: Canonical Forms

11.1 ⋆ 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.

11.2 ⋆ 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.

11.3 ⋆ Spring 2012 #7

Consider the following matrix as a linear transformation from $V \coloneqq \mathbb{C}^5$ 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.

11.4 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 $(x^2+1)^2(x^3+1)$.

11.5 Fall 2019 Final #9

Exhibit the rational and Jordan canonical forms for the following matrix $A \in M_4(\mathbb{C})$:

$$A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ -2 & -2 & 0 & 1 \\ -2 & 0 & -1 & -2 \end{pmatrix}.$$

11.6 Spring 2016 #7

Let $D = \mathbb{Q}[x]$ and let M be a $\mathbb{Q}[x]$-module such that

$$M \cong \frac{\mathbb{Q}[x]}{(x-1)^3} \oplus \frac{\mathbb{Q}[x]}{(x^2+1)^3} \oplus \frac{\mathbb{Q}[x]}{(x-1)(x^2+1)^5} \oplus \frac{\mathbb{Q}[x]}{(x+2)(x^2+1)^2}.$$

Determine the elementary divisors and invariant factors of M.

11.7 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 $P^{-1}AP = J$.

You should not need to compute P^{-1}.

c. Write down the minimal polynomial of A.

11.8 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

$$JCF_{\mathbb{Q}}(A) = J^1_{p-1} \oplus (p-1)J^1_{-1} = \left[\begin{array}{c|c|c|c|c|c} p-1 & 0 & 0 & \cdots & 0 & 0 \\ \hline 0 & -1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \ddots & \ddots & 0 \\ \hline 0 & 0 & 0 & \cdots & -1 & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 & -1 \end{array}\right].$$

- 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 $\min_{A,\mathbb{F}_p}(x) = (x+1)^2$.
  - 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

$$JCF_{\mathbb{F}_p}(A) = J_{-1}^2 \oplus (p-2)J_{-1}^1 = \left[\begin{array}{cc|c|c|cc} -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \ddots & \ddots & 0 \\ \hline 0 & 0 & 0 & \cdots & -1 & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 & -1 \end{array}\right].$$

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

$$P = [\mathbf{v}_1, \mathbf{x}, \mathbf{p}_1, \cdots, \mathbf{p}_{p-2}] = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 1 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

11.9 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}.

11.10 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.

11.11 Spring 2016 #1

Let

$$A = \begin{pmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{pmatrix} \in M_3(\mathrm{C}).$$

a. Find the Jordan canonical form J of A.

b. Find an invertible matrix P such that $P^{-1}AP = J$. You do not need to compute P^{-1}.

11.12 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.

11.13 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.

11.14 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.

11.15 Spring 2021 #1

Let m

$$A \coloneqq \begin{bmatrix} r & 1 & -1 \\ -6 & -1 & 2 \\ 2 & 1 & 1 \end{bmatrix} \in \mathrm{Mat}(3 \times 3, \mathbb{C}).$$

a. Find the Jordan canonical form J of A.

b. Find an invertible matrix P such that $J = P^{-1}AP$.

You should not need to compute P^{-1}

c. Write down the minimal polynomial of A.

11.16 Fall 2020 #5

Consider the following matrix:

$$B \coloneqq \begin{bmatrix} 1 & 3 & 3 \\ 2 & 2 & 3 \\ -1 & -2 & -2 \end{bmatrix}.$$

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.