Qual Algebra: Problems and Solutions

Compiled March 2023

Table of Contents

Contents

Та	able o	of Contents	2
1	Pre	face	14
2	Gro	up Theory: General	14
	2.1	Permutations	14
		2.1.1 Fall 2021 #1	14
	2.2	Cosets	15
		2.2.1 Spring 2020 #2	15
		2.2.2 Fall 2014 #6 \ldots	16
		2.2.3 Spring 2013 #3	16
	2.3	Burnside / Class Equation	17
		2.3.1 Spring 2019 #4	17
	2.4	Group Actions / Representations	20
		2.4.1 Spring 2017 #1	20
		2.4.2 Fall 2015 #1	$\overline{22}$
	2.5		23
		2.5.1 Spring 2021 #2	23
		2.5.2 Spring 2015 #1	24
	2.6	Unsorted / Counting Arguments	25
		2.6.1 Fall 2021 $\#2$	25
			26
		2.6.3 Spring 2012 #2	27
			29
			30
			32
3	Gro	oups: Group Actions	32
5	3.1	Fall $2012 \#1$	
	$3.1 \\ 3.2$		32 32
	$\frac{5.2}{3.3}$	Spring 2016 $\#5$	
	3.4		33
	$3.4 \\ 3.5$	Fall 2018 #2 \cdots	
	0.0	1 an 2010	00
4			36
	4.1		36
	4.2		37
	4.3		37
	4.4		38
	4.5	Fall 2014 #2 \ldots	38
	4.6		38
	4.7	Spring 2017 $\#2$	38

	4.8	Fall 201	7~#2 .	• • •										•	•	•••	•••	• •	•	•••	• •	•	• •	•	39
	4.9	Fall 2012	2~#2 .																						41
	4.10	Fall 201	3 #1 .																						41
	4.11	Fall 201) #2 .																						43
	4.12	Spring 2	$021 \ #3$																						46
		Fall 202																							46
		Fall 202																							46
5	Grou	ups: Clas	sificatio	on																					46
	5.1	Spring 2	020 #1																						46
	5.2	Spring 2	$019 \ #3$																						47
	5.3	Spring 2																							
	5.4	Fall 201																							
	5.5	Spring 2																							
		-r 0	//																						
6	Grou	ups: Sim																							50
	6.1	\star Fall 20	16 #7																						50
	6.2	Spring 2																							51
	6.3	Spring 2	014 #1																						53
	6.4	Fall 201	3 #1 ^{°°} .																						53
	6.5	Spring 2	$013 \ #4$																						53
	6.6	Fall 201																							53
7		nmutative																							54
	7.1	UFDs, F																							54
				012 -	ЦО																				54
			pring 2																						
			pring 2 all 201																						55
		7.1.2 H		7 #6	•									•	•				•						55 57
	7.2	7.1.2 H	all 201' pring 2	7 #6 017 ₇	#4	 	 	 	 	· ·	· ·	· ·	· ·	•	•••	· ·	 	· ·	•	 	 	•	 		55
	7.2	7.1.2 H 7.1.3 S Ideals (H	all 201' pring 2	7 #6 017 ₇ Maxir	#4 nal,	Pr	 ope	 r, P	 rinc	ipal	 , et	· · · · c) ·	· · · ·	• •		 	· ·	· · · ·		· ·	· · ·		 		55 57
	7.2	7.1.2 H 7.1.3 S Ideals (H 7.2.1 H	all 201 pring 2 Prime, 1	7 #6 017 ₇ Maxir 1 #5	#4 nal, #a	Pr lgeb	 ope ora/	· · r, P 'qua	rinc l/st	ipal uck	 , et	 c) .	· · · ·	• •	· ·	 	 	· · · ·		 	· · · ·	•	· ·		55 57 58
	7.2	7.1.2 H 7.1.3 S Ideals H 7.2.1 H 7.2.2 H	Vall 201 pring 2 Prime, 1 Vall 202	7 #6 017 ₇ Maxir 1 #5 3 #3	#4 nal, #a	Pr lgeb	ope ora/	r, P qua	rinc l/st	ipal uck	, et		· · · · · · ·	• •	•	· · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · ·		· · · · · ·	· · · · · ·		 		55 57 58 58
	7.2	7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H	Vall 201pring 2Prime, 1Vall 202Vall 2013	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8	#4 nal, #a	Pr lgeb	 ope ora/ 	 r, P 'qua 	rinc l/st	ipal uck	., et	 c) . 	· · · · · · · ·	• • • • • •	· •	· · · · · · · · · · · · · · · · · · ·	· · · · · · · ·	· · · · · ·		· · · · · ·	· · · · · · · · · · · · · · · · · · ·		· · · · · ·		55 57 58 58 58 59
	7.2	7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H	all 201' pring 2 Prime, 1 'all 202 'all 201 'all 201 'all 201	7 #6 017 ₇ Maxir 1 #5 3 #3 4 #8 4 #7	#4 nal, #a	Pro lgeb	 ope ora/ 	· · · r, P /qua · · ·	rinc l/st	ipal uck	., et 		· · · · · · · · ·	• • • • • •	· •	 . .<	 . .<	· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·		55 57 58 58 59 59
	7.2	7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S	all 201 ⁴ pring 2 Prime, 1 Vall 202 Vall 201 Vall 201 Vall 201 Vall 201 Vall 201 Vall 201	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #7 019 $_{7}$	#4 nal, #a #6	Proligeb	• • • ope ora/ • • •	 r, P /qua 	$\frac{1}{st}$	ipal uck 	, et , et	· · · c) · · · · ·	· · · · · · · · · · ·	- · · - · · - · ·		 . .<	 . .<	· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · ·	· · · · · · · · · · · ·		· · · · · · · · ·		55 57 58 58 59 59 59
	7.2	7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S	all 201 ⁴ pring 2 Prime, 1 Call 202 Call 201 Call 201 Call 201 Call 201 pring 2 pring 2	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #8 4 #7 019 $_{7}$ 018 $_{7}$	#4 nal, #a #6 #8	Pr lgeb	 ope ora/ 	 r, P qua 	$\frac{1}{st}$	ipal uck 	, et , et	c) . 	· · · · · · · · · · · ·	· · ·		 . .<	 . .<	· · · · · · · · · · · · · · · · · · ·	· · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·	· · ·	55 57 58 58 59 59 59 60
		7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S Zero Div	all 201 [°] pring 2 Prime, 1 `all 202 `all 201 [°] `all 201 [°] `all 201 [°] all 201 [°] pring 2 pring 2 risors a	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #7 019 $_{7}$ 018 $_{7}$ nd Ni	#4 nal, #a #6 #8 ilpo	Proliget	ope ora/ 	 r, P qua 	rinc l/st	ipal uck 	, et	c) . 	· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	 . .<	 . .<	· · · · · · · · · · · · · · · · · · ·	• • • • • • •	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · ·		· · · · · · · · · · · ·	· · · ·	55 57 58 59 59 59 60 63 65
		7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S Zero Div 7.3.1	all 201 [°] pring 2 Prime, 1 Call 202 [°] call 201 [°] call 201 [°] call 201 [°] pring 2 pring 2 risors au pring 2	7 #6 017 $_{7}$ Maxin 1 #5 3 #3 4 #8 4 #7 019 $_{7}$ 018 $_{7}$ nd Ni 014 $_{7}$	#4 nal, #a #6 #8 ilpo #5	Pr lget	ope pra/ 	 r, P qua 	rinc l/st	 ipal uck 	 , et 		· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	 . .<	••••••	· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	55 57 58 59 59 59 60 63 63 65 65
		7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S Zero Div 7.3.1 7.3.2 S	all 201 [°] pring 2 Prime, 1 Call 202 Call 201 [°] Call 201 [°] Call 201 [°] Call 201 [°] Call 201 [°] pring 2 pring 2 pring 2 pring 2 pring 2	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #7 019 $_{7}$ 018 $_{7}$ 018 $_{7}$ 018 $_{7}$ 014 $_{7}$ 021 $_{7}$	#4 mal, #a = 46 #6 #8 llpo = 45 #5 #5 #5 #5 #5 #5 #5 #5 #5 #5 #5 #5 #5	Pr lget	 ope ora/ 	 r, P qua 	rinc 1/st	ipal uck	, et 		· · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·	 . .<		· · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · ·	· · · · ·	55 57 58 59 59 60 63 65 65
	7.3	7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S Zero Div 7.3.1 7.3.2 S 7.3.3 H	all 201 [°] pring 2 Prime, 1 Call 202 Call 201 [°] Call 201 [°] Call 201 [°] Call 201 [°] pring 2 pring 2 pring 2 pring 2 Call 201 [°]	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #7 019 $_{7}$ 018 $_{7}$ 018 $_{7}$ 018 $_{7}$ 014 $_{7}$ 021 $_{7}$ 8 #7	$#4 \\ mal, #a \\ #a \\ #6 \\ #8 \\ llpo \\ #5 \\ #5 \\ #5$	Pr lget	 ope ora/ 	 r, P /qua 	rinc 1/st	ipal uck 	, et		· · · · · · · · · · · · · · · · · · ·			· ·	· ·	 . .<	• • • • • • • • • •	· ·	· ·	· · · · · ·	· · · · · · · · · · · · · · · · · ·	· · · · ·	55 57 58 59 59 60 63 65 65 65 65
		7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S Zero Div 7.3.1 S 7.3.3 H Zorn's L	all 201 [°] pring 2 Prime, 1 Call 202 [°] call 201 [°] call 201 [°] call 201 [°] pring 2 pring 2 pring 2 pring 2 pring 2 call 201 [°] call 201 [°]	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #7 019 $_{7}$ 018 $_{7}$ nd Ni 014 $_{7}$ 021 $_{7}$ 8 #7	#4 nal, #a #6 #8 lpo #5 #5	Pr lget	 ope ora/ 	 r, P qua 	rinc l/st	ipal uck 	, et		· · · · · · · · · · · · · · · · ·			· · · · · ·	· · · · · ·	 . .<		· · · · · ·	· · · · · ·	· · · · · ·	· ·	· · · · · · · · · · · · · · · · · · ·	55 57 58 59 59 60 63 65 65 65 65 66 70
	7.3	7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S 7.2.6 S 7.3.1 S 7.3.2 S 7.3.3 H Zorn's L 7.4.1	all 201 [°] pring 2 Prime, 1 Call 202 Call 201 [°] Call 201 [°] Call 201 [°] pring 2 pring 2 pring 2 pring 2 Call 201 [°] call 201 [°] call 201 [°]	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #7 019 $_{7}$ 018 $_{7}$ nd Ni 014 $_{7}$ 021 $_{7}$ 8 #7 3 #4	#4 mal, #a #6 #8 ilpo #5 #5	Pr lget	ope ora/ · · · · · · · · · · · ·	 r, P qua 	rinc 1/st	ipal uck 	, et		· ·			· · · · · ·	· · · · · ·	 . .<		· · · · · ·	 . .<	· · · · · · ·	· · · · · ·	· · · · · · · · · · · · · · · · · · ·	55 57 58 59 59 60 63 65 65 65 66 70 70
	7.3	7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S 7.3.1 S 7.3.2 S 7.3.3 H Zorn's L 7.4.1 7.4.2 H	all 201' pring 2 Prime, 1 'all 202 'all 201	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #7 019 $_{7}$ 018 $_{7}$ 018 $_{7}$ 014 $_{7}$ 021 $_{7}$ 8 #7 3 #4 5 #3	#4 nal, #a #6 #8 Ilpo #5 #5	Pr lgeb		 r, P /qua 	rinc 1/st	ipal uck 	, et					· · · · ·	· · · · · ·	 . .<	· · · · · · · · · · · · ·	· · · · · ·	 . .<	· · · · · · · · · · · · · · · · · · ·	 . .<	· · · · · · · · · · · · · · · · · · ·	55 57 58 59 59 60 63 65 65 65 66 70 70 70
	7.3	7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S 7.2.7 S 7.2.8 S 7.2.9 S 7.2.5 S 7.2.6 S 7.3.1 S 7.3.3 H Zorn's L T 7.4.1 H 7.4.3 S	all 201 [°] pring 2 Prime, I all 202 [°] all 201 [°] all 201 [°] all 201 [°] all 201 [°] pring 2 pring 2 pring 2 all 201 [°] emma all 201 [°] all 201 [°] all 201 [°] all 201 [°] all 201 [°]	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #7 019 $_{7}$ 019 $_{7}$ 018 $_{7}$ 014 $_{7}$ 021 $_{7}$ 8 #7 3 #4 5 #3 015 $_{7}$	#4 nal, #a #6 #8 llpo #5 #5 #5	Pr lget	 ope ora/ 	 r, P qua 	rinc 1/st	ipal uck 	, et					· · · · · ·	· · · · · ·	 . .<	· · · · · · · · · · · · · · · · · · ·	 . .<	· · · · · ·	· · · · · · · · · · · · · · · · · · ·	 . .<	· · · · · · · · · · · · · · · · · · ·	$55 \\ 57 \\ 58 \\ 59 \\ 59 \\ 60 \\ 63 \\ 65 \\ 65 \\ 65 \\ 66 \\ 70 \\ 70 \\ 70 \\ 71 \\$
	7.3	7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S 7.2.7 S 7.2.8 S 7.2.9 S 7.2.6 S 7.3.1 S 7.3.2 S 7.3.3 H Zorn's L S 7.4.1 H 7.4.3 S 7.4.4 S	all 201 [°] pring 2 Prime, 1 Call 202 Call 201 [°] Call 201 [°] Call 201 [°] Call 201 [°] pring 2 pring 2 Call 2013 Call 2013 Call 2013 Call 2014 Call 2014 Call 2014 Call 2015 Call 2017 Call	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #7 019 $_{7}$ 018 $_{7}$ 018 $_{7}$ 014 $_{7}$ 021 $_{7}$ 3 #4 5 #3 015 $_{7}$ 013 $_{7}$	#4 nal, #a #6 #8 lpo #5 #5 #5 #7 #1	Proliget	· · · · · · · · · · · · · · · · · · ·	· · · r, P qua · · · · · · · · · · · · · · · · ·	rinc l/st	ipal uck 	, et 					· ·	· ·	 . .<		 . .<	· ·	· · · · · · · · · · · · · · · · · · ·	· · · · · ·	· · · · · · · · · · · · · · · · · · ·	$55 \\ 57 \\ 58 \\ 59 \\ 59 \\ 59 \\ 60 \\ 63 \\ 65 \\ 65 \\ 65 \\ 66 \\ 70 \\ 70 \\ 70 \\ 71 \\ 72$
	7.3 7.4	7.1.2 H 7.1.3 S Ideals (H 7.2.1 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S 7.3.1 S 7.3.2 S 7.3.3 H 7.4.1 H 7.4.2 H 7.4.3 S 7.4.4 S 7.4.5 H	all 201' pring 2 Prime, 1 'all 202 'all 201	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #7 019 $_{7}$ 018 $_{7}$ 018 $_{7}$ 014 $_{7}$ 021 $_{7}$ 8 #7 3 #4 5 #3 015 $_{7}$ 013 $_{7}$ 9 #6	$#4 \\ mal, #a \\ #6 \\ #8 \\ llpo \\ #5 \\ #5 \\ #7 \\ #1$	Prilget		· · · r, P qua · · · · · · · · · · · · · · · · · · ·	rinc 1/st	ipal uck 	, et , et , , - , - , - , - , - , - , - , - ,					 . .<	 · · · ·	 . .<		 . .<	· ·	· · · · · · · · · · · · · · · · · · ·	· ·	· · · · · · · · · · · · · · · · · · ·	$55 \\ 57 \\ 58 \\ 59 \\ 59 \\ 59 \\ 59 \\ 60 \\ 63 \\ 65 \\ 65 \\ 66 \\ 70 \\ 70 \\ 70 \\ 70 \\ 71 \\ 72 \\ 73 \\$
	7.3	7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S 7.2.7 S 7.2.8 H 7.2.5 S 7.2.6 S 7.2.7 S 7.3.1 S 7.3.3 H Zorn's L T 7.4.1 H 7.4.2 H 7.4.3 S 7.4.4 S 7.4.5 H Noether S	all 201 [°] pring 2 Prime, I all 202 [°] all 201 [°] all 201 [°] all 201 [°] all 201 [°] pring 2 pring 2 pring 2 all 201 [°] all 201 [°] all 201 [°] pring 2 pring 2 all 201 [°] all 201 [°] all 201 [°] an Rin	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #7 019 $_{7}$ 019 $_{7}$ 018 $_{7}$ 014 $_{7}$ 021 $_{7}$ 8 #7 3 #4 5 #3 015 $_{7}$ 013 $_{7}$ 9 #6 gs	#4 nal, #a #6 #8 llpo #5 #5 #7 #1	Prilgek	 ope ora/ 	· · · r, P qua · · · · · · · · · · · · · · · · · · ·	rinc 1/st	ipal uck 	, et					· ·	· ·	 . .<		 . .<	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· ·	· · · · · · · · · · · · · · · · · · ·	$55 \\ 57 \\ 58 \\ 59 \\ 59 \\ 60 \\ 63 \\ 65 \\ 65 \\ 65 \\ 66 \\ 70 \\ 70 \\ 70 \\ 70 \\ 71 \\ 72 \\ 73 \\ 75 \\ $
	7.3 7.4	7.1.2 H 7.1.3 S Ideals (H 7.2.1 H 7.2.2 H 7.2.3 H 7.2.4 H 7.2.5 S 7.2.6 S Zero Div 7.3.1 7.3.2 S 7.3.3 H Zorn's L 7.4.1 7.4.3 S 7.4.4 S 7.4.5 H Noether 7.5.1	all 201' pring 2 Prime, 1 'all 202 'all 201 'all 2014 pring 2 pring 2 'all 2013 'all 2014 emma 'all 2014 pring 2 'all 2014 pring 2 'all 2014 pring 2 'all 2014 pring 2 'all 2014	7 #6 017 $_{7}$ Maxir 1 #5 3 #3 4 #8 4 #7 019 $_{7}$ 018 $_{7}$ 018 $_{7}$ 014 $_{7}$ 021 $_{7}$ 3 #4 5 #3 015 $_{7}$ 013 $_{7}$ 0 #6 gs 5 #4	#4 nal, #a #6 #8 lpo #5 #5 #7 #1	Proliget	· · · · · · · · · · · · · · · · · · ·	· · · r, P qua · · · · · · · · · · · · · · · · · · ·	rinc l/st	ipal uck 	, et 					· ·	 · · · ·			 · ·<	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· ·		$55 \\ 57 \\ 58 \\ 59 \\ 59 \\ 59 \\ 59 \\ 60 \\ 63 \\ 65 \\ 65 \\ 66 \\ 70 \\ 70 \\ 70 \\ 70 \\ 71 \\ 72 \\ 73 \\$

	7.6	Simple	m Rings
		7.6.1	Fall 2017 #5
		7.6.2	Spring 2016 #8
	7.7	Unsort	ed
		7.7.1	Fall 2019 #3
		7.7.2	Spring 2018 #5
		7.7.3	Spring 2014 $\#6$
8	Galo	ois Theo	bry 83
	8.1	Genera	al Galois Extensions
		8.1.1	Fall 2021 #4
		8.1.2	Fall 2020 #4
		8.1.3	Fall 2019 Midterm #9 88
		8.1.4	Fall 2019 Midterm #10 86
		8.1.5	Fall 2019 Midterm #8 8 8 8
		8.1.6	Fall 2019 Midterm #7 87 87
		8.1.7	Spring 2012 #4
		8.1.8	Fall 2013 #5
		8.1.9	Fall 2012 #4
	8.2	Galois	Groups: Concrete Computations
		8.2.1	Exercise: $G(x^2-2)$
		8.2.2	Exercise: $G(x^p - 2)$ 89
		8.2.3	Fall 2020 #3
		8.2.4	Spring 2021 #4
		8.2.5	Fall 2019 Midterm #6
		8.2.6	Spring 2018 #2
		8.2.7	Spring 2020 #4
		8.2.8	Spring 2017 #8
		8.2.9	Fall 2016 #4
		8.2.10	Spring 2016 #2
		8.2.11	Fall 2015 #5
		8.2.12	Spring 2015 #5
		8.2.13	Fall 2014 #3
		8.2.14	Fall 2013 #6
		8.2.15	Spring 2014 #4
		8.2.16	Spring 2013 #8
	8.3	Galois	Groups: Indirect Computations / Facts
		8.3.1	Fall 2019 #7
		8.3.2	Fall 2018 #3
		8.3.3	Spring 2018 #3
		8.3.4	Fall 2017 #4
		8.3.5	Spring 2017 #7
		8.3.6	Spring 2016 #6
		8.3.7	Fall $2015 \# 6$
		8.3.8	Fall 2014 $\#1$
		8.3.9	Spring $2013 \#7$
		8.3.10	Fall 2012 #3

	8.4	pth Ro	ots and $x^{p^k} - x$					•															108
		8.4.1	Spring 2021 #7																				108
		8.4.2	Fall 2019 #4																				110
		8.4.3	Spring 2019 #2																				111
		8.4.4	\star Fall 2016 #5 $$.					•						•									113
		8.4.5	\star Fall 2013 #7 $$.																				114
	8.5	Genera	l Field Extensions																				114
		8.5.1	Spring 2020 $\#3$					•															114
		8.5.2	Spring 2012 #1																				115
		8.5.3	Spring 2019 #8																				115
		8.5.4	Fall 2017 $\#3$					•															117
		8.5.5	Spring 2015 $\#2$					•						•									117
		8.5.6	Spring 2014 #3					•	• •					•				• •	•				117
9	Мос	lules																					117
	9.1		lators																				
	0.1		Fall 2021 #6																				
			Spring 2017 $\#5$																				
	9.2		and the Structure																				
	0.2		\star Fall 2019 #5																				
			* Spring 2019 $\#5$.																				
			* Spring 2020 #6.																				
			Spring 2012 #5																				
			Fall 2019 Final #3																				
			Fall 2019 Final #4																				
			Fall 2019 Final $\#5$																				
			Fall 2019 Final $\#6$																				
			Fall 2019 Final $\#7$																				
			Fall 2019 Final $\#10^{-10}$																				
			Fall 2020 $\#7$																				
	9.3		Insorted																				
		· · · ·	Spring 2017 #3																				
			Spring 2020 $\#5$																				
			Fall 2018 $\#6^{''}$																				
			Fall 2019 Final $#2$																				
			Spring 2018 #6 ["]																				
			Spring 2018 $\#7$																				
			Fall 2016 #6																				
			Spring 2016 #4																				
			Spring 2015 #8																				
			Fall 2012 $\#6$																				
			Fall 2019 Final #1																				
			Fall 2020 $\#6$																				
10	Line	ar Algel	ora: Diagonalizabili	tv																			137
-0			17 #7 · · · · · · · ·	- - -																			
			$2015 \#3 \dots$																				
			$16 \#2 \dots$																				
	10.0	1 an 20.	$T^2 \cdots \cdots$	• •	• •	• •	• •	•	• •	• •	• •	• •	• •	•	•••	• •	•	• •	•	• •	•	• •	100

10.4 Spring 2019 #1	 . 139
11 Linear Algebra: Misc	141
11.1 \star Spring 2012 #6	 . 141
11.2 \star Spring 2014 #7	 . 141
11.3 Fall 2012 #7	 . 141
11.4 Fall 2012 #8	 . 142
11.5 Fall 2012 #5	 . 142
11.6 Fall 2015 #7	 . 142
11.7 Fall 2014 $\#4$. 142
11.8 Fall 2015 #8	 . 143
11.9 Fall 2018 $\#4$	
11.10Fall 2018 $\#5$	
11.11Fall 2019 #8	
11.12Spring 2013 #6	
11.13Fall 2020 #8	
	 . 100
12 Linear Algebra: Canonical Forms	151
12.1 Fall 2021 #3 \ldots \ldots \ldots \ldots \ldots	
$12.2 \star \text{Spring } 2012 \# 8 \dots \dots$	
$12.3 \star \text{Spring } 2020 \# 8 \dots \dots$	
12.4 \star Spring 2012 #7	
12.5 Fall 2019 Final #8 \ldots	
12.6 Fall 2019 Final $\#9$	
12.7 Spring 2016 #7	
12.8 Spring 2020 $\#7$. 154
12.9 Spring 2019 $\#7$. 154
12.10Spring 2018 #4 \ldots	 . 158
12.11Spring 2017 #6 \ldots	 . 158
12.12Spring 2016 #1	 . 158
12.13Spring 2015 #6	 . 159
12.14Fall 2014 #5	 . 160
12.15Spring 2013 #5 \ldots	 . 160
12.16 Spring $2021 \# 1 \dots $. 160
12.17Fall 2020 #5	 . 163
12 Future Durchlaure	163
13 Extra Problems 13.1 Linear Algebra	
13.2 Galois Theory	
13.3 Commutative Algebra	
13.4 Group Theory	
13.4.1 Centralizing and Normalizing	
13.4.2 Primes in Group Theory \ldots \ldots \ldots \ldots \ldots \ldots	
13.4.3 p-Groups	
13.4.4 Symmetric Groups \ldots \ldots \ldots \ldots \ldots \ldots	
13.4.5 Alternating Groups $\dots \dots \dots$	
13.4.6 Dihedral Groups \dots	
13.4.7 Other Groups \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots	 . 170

	13.4.8 Classification	70
	13.4.9 Group Actions	70
	13.4.10 Series of Groups	70
	13.4.11 Misc	
	13.4.12 Nonstandard Topics	
13.5	Ring Theory	
	13.5.1 Basic Structure	
	13.5.2 Ideals	
	13.5.3 Characterizing Certain Ideals	
	13.5.4 Misc	
13.6	Field Theory	
	Galois Theory	
10.1	13.7.1 Theory	
	13.7.2 Computations	
13.8	Modules and Linear Algebra	
	Linear Algebra	
10.0		
14 Eve	1 More Algebra Questions	77
	Groups	77
	14.1.1 Question 1.1	77
	14.1.2 Question 1.2	77
	14.1.3 Question 1.3	77
	14.1.4 Question 1.4	77
	14.1.5 Question 1.5	77
	14.1.6 Question 1.6	78
	14.1.7 Question 1.7	78
	14.1.8 Question 1.8	78
	14.1.9 Question 1.9	78
	14.1.10 Question 1.10	78
	14.1.11 Question 1.11	78
	14.1.12 Question 1.12	78
	14.1.13 Question 1.13	79
	14.1.14 Question 1.14	79
	14.1.15 Question 1.15	79
	14.1.16 Question 1.16	79
	14.1.17 Question 1.17	79
	14.1.18 Question 1.18	79
	14.1.19 Question 1.19	79
	14.1.20 Question 1.20	79
	14.1.21 Question 1.21	80
	14.1.22 Question 1.22	80
	14.1.23 Question 1.23	80
	14.1.24 Question 1.24	80
	14.1.25 Question 1.25	80
	14.1.26 Question 1.26	
	14.1.27 Question 1.27	
	14.1.28 Question 1.28	80
	14.1.29 Question 1.29	81

	14.1.30 Question 1.30	181
	14.1.31 Question 1.31	
	•	
	14.1.32 Question 1.32	
	14.1.33 Question 1.33	
	14.1.34 Question 1.34	181
	14.1.35 Question 1.35	181
	14.1.36 Question 1.36	182
	14.1.37 Question 1.37	
	14.1.38 Question 1.38	
	14.1.39 Question 1.39	
	•	
	14.1.40 Question 1.40	
	14.1.41 Question 1.41	
	14.1.42 Question 1.42	
	14.1.43 Question 1.43	183
	14.1.44 Question 1.44	183
14.2	Classification of Finite groups	183
	14.2.1 Question 2.1	
	14.2.2 Question 2.2	
	14.2.3 Question 2.3	
	•	
	14.2.4 Question 2.4	
	14.2.5 Question 2.5	
	14.2.6 Question 2.6	
	14.2.7 Question 2.7	184
	14.2.8 Question 2.8	184
	14.2.9 Question 2.9	184
	14.2.10 Question 2.10	
	14.2.11 Question 2.11	
	14.2.12 Question 2.12	
	14.2.13 Question 2.13	
	•	
	14.2.14 Question 2.14	
	14.2.15 Question 2.15	
	14.2.16 Question 2.16	
	14.2.17 Question 2.17	185
	14.2.18 Question 2.18	185
	14.2.19 Question 2.19	185
	14.2.20 Question 2.20	
14.3	Fields and Galois Theory	
11.0	14.3.1 Question 3.1	
	•	
	14.3.2 Question 3.2	
	14.3.3 Question 3.3	
	14.3.4 Question 3.4	186
	14.3.5 Question 3.5	186
	14.3.6 Question 3.6	186
	14.3.7 Question 3.7	186
	14.3.8 Question 3.8	
	14.3.9 Question 3.9	
	14.3.10 Question 3.10	
	14.3.11 Question 3.11	
	14.0.11 QUESHOIL 0.11	191

14.3.12 Question 3.12	
14.3.13 Question 3.13	37
14.3.14 Question 3.14	37
14.3.15 Question 3.15	
14.3.16 Question 3.16	
14.3.17 Question 3.17	
14.3.18 Question 3.18	
14.3.19 Question 3.19	
14.3.20 Question 3.20	
14.3.21 Question 3.21	
14.3.22 Question 3.22	
14.3.23 Question 3.23	
14.3.24 Question 3.24	
14.3.24 Question 3.24 16.14 $14.3.25$ Question 3.25 18	
14.3.26 Question 3.26	
14.3.27 Question 3.27	
14.3.28 Question 3.28	
14.3.29 Question 3.29	
14.3.30 Question 3.30	
14.3.31 Question 3.31	
$14.3.32 \text{ Question } 3.32 \dots \dots$	
$14.3.33 \text{ Question } 3.33 \dots $)0
14.3.34 Question 3.34)0
14.3.35 Question 3.35)0
14.3.36 Question 3.36)0
14.3.37 Question 3.37)0
14.3.38 Question 3.38	
14.3.39 Question 3.39	
14.3.40 Question 3.40	
14.3.41 Question 3.41	
$14.3.42 \text{ Question } 3.42 \dots \dots 19$	
$14.3.43 \text{ Question } 3.43 \dots \dots 19$	
14.3.44 Question 3.44	
$14.3.45 \text{ Question } 3.45 \dots \dots 19$	
$14.3.46 \text{ Question } 3.46 \dots \dots$	
$14.3.47 \text{ Question } 3.47 \dots 19$	
· · · · · · · · · · · · · · · · · · ·	
14.3.48 Question 3.48	
14.3.49 Question 3.49	
14.3.50 Question 3.50	
$14.3.51 \text{ Question } 3.51 \dots \dots$	
$14.3.52 \text{ Question } 3.52 \dots \dots$	
$14.3.53 \text{ Question } 3.53 \dots \dots$	
$14.3.54 \text{ Question } 3.54 \dots \dots$	
14.3.55 Question 3.55)3
14.3.56 Question 3.56)3
14.3.57 Question 3.57)3
14.3.58 Question 3.58)3
14.3.59 Question 3.59)3

		Question 3														
	14.3.61	Question 3	.61 .				 	 			•	 		 •		. 193
	14.3.62	Question 3	.62 .				 	 			•	 				. 194
	14.3.63	Question 3	.63 .				 	 				 		 		. 194
		Question 3														
		Question 3														
		Question 3														
		Question 3														
		Question 3														
		Question 3														
		Question 3														
		Question 3														
		Question 3														
		•														
		Question 3														
		Question 3														
		Question 3														
		Question 3														
		Question 3														
		Question 3														
14.4		l Forms														
		Question 4														
	14.4.2	Question 4	.2 .		 •	•••	 	 	•••	•••	•	 	•••	 •		. 196
	14.4.3	Question 4	.3 .				 	 		•••	•	 		 		. 196
	14.4.4	Question 4	.4 .				 	 			•	 		 		. 196
	14.4.5	Question 4	.5 .				 	 				 		 		. 196
	14.4.6	Question 4	.6 .				 	 			•	 				. 196
	14.4.7	Question 4	.7 .				 	 				 		 		. 197
	14.4.8	Question 4	.8 .				 	 			•	 		 		. 197
		Question 4														
		Question 4														
		Question 4														
		Question 4														
		Question 4														
		Question 4														
		Question 4														
		Question 4														
		Question 4														
		Question 4														
		•														
		Question 4														
		Question 4														
		Question 4														
14.5		es and Line		<u> </u>												
		Question 5														. 199
		Question 5														
		Question 5														
		Question 5														. 199
	14.5.5	Question 5														. 199
	14.5.6	Question 5	.6 .				 	 		•••	•	 		 •••		. 199

	14.5.7	Question	5.7 .	•	 	•	 •	 		 	•	 			 		199
	14.5.8	Question	5.8 .		 		 •	 		 		 		•	 		200
	14.5.9	Question	5.9 .		 			 		 		 			 		200
	14.5.10	Question	5.10 .		 			 		 		 			 		200
		Question															
		Question															
		Question															
		Question															
		Question															
		Question															
		Question															
		•															
		Question															
		Question															
1.1.0		Question															
14.6	0																
		Question															
		Question															
		Question															
	14.6.4	Question	6.4 .	•	 • •	•	 •	 	 •	 	•	 		•	 	•	202
	14.6.5	Question	6.5 .	•	 	•	 	 		 	•	 			 		202
	14.6.6	Question	6.6 .		 			 		 		 			 		202
	14.6.7	Question	6.7 .		 		 	 		 		 			 		202
	14.6.8	Question	6.8 .		 			 		 		 			 		202
	14.6.9	Question	6.9 .		 		 	 		 		 			 		202
	14.6.10	Question	6.10 .		 		 	 		 		 			 		202
		Question															
		Question															
		Question															
		Question															
		Question															
		Question															
		Question															
		Question															
		•															
		Question															
		Question															
		Question															
		Question															
		Question															
		Question															
		Question															
		Question															
	14.6.27	Question	6.27 .	•	 		 •	 	 •	 	•	 		•	 	•	205
	14.6.28	Question	6.28 .	•	 			 		 		 			 		205
	14.6.29	Question	6.29 .		 			 		 		 		•	 		205
	14.6.30	Question	6.30 .		 		 	 		 		 			 		205
	14.6.31	Question	6.31 .		 			 		 		 			 		205
		Question															
		Question															
	-	•															

	14.6.34 Questio	n 6.34 .			 			 							206
	14.6.35 Questio	n 6.35 .			 			 							206
	14.6.36 Questio	n 6.36 .			 			 							206
	14.6.37 Question	n 6.37 .			 			 							206
	14.6.38 Question	n 6.38 .			 			 							206
	14.6.39 Question														
	14.6.40 Question														
	14.6.41 Question														
	14.6.42 Questio														
	14.6.43 Question														
	14.6.44 Questio														
	14.6.45 Questio														
	14.6.46 Questio														
	14.6.47 Questio														
	14.6.48 Questio														
	14.6.49 Questio														
	14.6.50 Questio														
	14.6.51 Questio														
	14.6.52 Questio														
147	Modules														
14.7	14.7.1 Question														
	14.7.1 Question 14.7.2 Question														
	14.7.2 Questio 14.7.3 Questio														
	•														
	14.7.4 Question														
	14.7.5 Question														
	14.7.6 Question														
	14.7.7 Question														
	14.7.8 Question														
	14.7.9 Question														
14.0	14.7.10 Question														
14.8	Representation	•													
	14.8.1 Question														
	14.8.2 Question														
	14.8.3 Question														210
	14.8.4 Question														210
	14.8.5 Question														210
	14.8.6 Question														210
	14.8.7 Question														210
	14.8.8 Question														211
	14.8.9 Questio														211
	14.8.10 Question														
	14.8.11 Question														
	14.8.12 Question														
	14.8.13 Questio														
	14.8.14 Questio														
	14.8.15 Questio														
	$14.8.16\mathrm{Questio}$														
	14.8.17 Question	n 8.17 .			 			 							212

	14.8.180	Juestion	8.18					 		 									212
	14.8.190	Juestion	8.19					 		 									212
	14.8.200	Question	8.20					 		 									212
	14.8.21 @	Juestion	8.21					 		 									212
	14.8.22 0	Question	8.22					 		 									212
	14.8.23 0	Juestion	8.23					 		 									213
	14.8.24 0	Juestion	8.24					 		 									213
	14.8.250	Question	8.25					 		 								. :	213
	14.8.260	Juestion	8.26					 		 								. :	213
	14.8.27 0	Juestion	8.27					 		 									213
	14.8.280	Juestion	8.28					 		 									213
	14.8.290	Juestion	8.29					 		 									213
	14.8.300	Juestion	8.30					 		 									214
	14.8.31 0	Juestion	8.31.					 		 									214
	14.8.320	Juestion	8.32					 		 									214
	14.8.330	Juestion	8.33			•	 •	 		 	•				 •				214
	14.8.340	Juestion	8.34			•	 •	 		 	•				 •				214
	14.8.350	Juestion	8.35			•	 •	 		 	•				 •				214
	14.8.360	Juestion	8.36			•	 •	 		 	•				 •				214
	14.8.370	Juestion	8.37			•		 		 	•				 •				215
14.9	Categori	les and F	Juncto	ors		•		 		 	•				 •				215
	14.9.1	Juestion	9.1			•		 		 	•				 •				215
	14.9.2	Juestion	9.2					 		 	•				 •				215
	14.9.3	Juestion	9.3			•	 •	 	•	 	•		 •	 •	 •	•	 •		215

1 | Preface

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

- Paco Adajar
- Swaroop Hegde

Many other solutions contain input and ideas from other graduate students and faculty members at UGA, along with questions and answers posted on Math Stack Exchange or Math Overflow. Any and all mistakes are surely my own!

2 | Group Theory: General

2.1 Permutations

2.1.1 Fall 2021 #1

Let G be a group. An automorphism $\varphi: G \to G$ is called *inner* if the automorphism is given by conjugation by a fixed group element g, i.e.,

$$\varphi = \varphi_q : h \mapsto ghg^{-1}.$$

- a. Prove that the set of inner automorphisms forms a normal subgroup of the group of all automorphisms of G.
- b. Give an example of a finite group with an automorphism which is not inner.
- c. Denote by S_n the group of permutations of the set $\{1, \ldots, n\}$. Suppose that $g \in S_n$ sends i to g_i for $i = 1, \ldots, n$. Let (a, b) denote as usual the cycle notation for the transposition which permutes a and b. For $i \in \{1, \ldots, n-1\}$, compute $\varphi_g((i, i+1))$.
- d. Suppose that an automorphism $\varphi \in \text{Aut}(S_n)$ preserves cycle type, i.e., that for every element s of S_n , s and $\varphi(s)$ have the same cycle type. Show that φ is inner.

Hint: Consider the images of generators $\varphi((1,2)), \varphi((2,3)), \cdots, \varphi((n-1,n)).$

2.2 Cosets

2.2.1 Spring 2020 #2

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

Concepts Used:

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

Strategy:

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

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

$$hN = h^{1}N$$

= $h^{ns+mt}N$
= $h^{ns}N \cdot h^{mt}N$
= $(h^{n}N)^{s} \cdot (h^{t}N)^{m}$
= $(eN)^{s} \cdot N$
= N ,

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

2.2.2 Fall 2014 #6

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

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

Concepts Used:

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

Strategy:

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

Solution:

- $H \cap K \le H \le G \implies [G: H \cap K] = [G: H][H: H \cap K]$
- So it suffices to show $[H: H \cap K] \leq [G:K]$
- Write $H/H \cap K = \{h_1J, \cdots, h_mJ\}$ as distinct cosets where $J \coloneqq H \cap J$.
- Then $h_i J \neq h_j J \iff h_i h_j^{-1} \notin J = H \cap K$.
- *H* is a subgroup, so $h_i h_j^{-1} \in H$ forces this not to be in *K*.
- But then $h_i K \neq h_j K$, so these are distinct cosets in G/K.
- So $\#G/K \ge m$.

2.2.3 Spring 2013 #3

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

Clean up, sketchy argument.

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

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

• Taking cardinalities,

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

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

2.3 Burnside / Class Equation

2.3.1 Spring 2019 #4

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

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

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

- b. State the class equation for a finite group.
- c. Using the class equation (or otherwise) show that the probability in part (a) is at most

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

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

Warning 2.3.1

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

Concepts Used:

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

Strategy:

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

Proof (Part a).

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

$$A \coloneqq \left\{ (g,h) \in G \times G \mid [g,h] = 1 \right\} \subseteq \Omega.$$

• Note that the slices are centralizers:

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

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

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

which is the **conjugacy class** of g. In particular, the number of orbits is the number of conjugacy classes.

- What are the fixed points?

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

which are the elements of G that commute with g, which is isomorphic to A_q .

• Identifying centralizers with fixed points,

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

• Apply Burnside

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

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

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

• Compute probability:

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

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

Proof (Part c).

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

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

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

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

$$g \notin Z(G) \implies \sharp Z(g) \le \frac{1}{2} \sharp G,$$

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

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

• Use these facts to calculate:

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

Redo part c

2.4 Group Actions / Representations

2.4.1 Spring 2017 #1

Let G be a finite group and $\pi: G \to \operatorname{Sym}^*(G)$ 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.

A Warning 2.4.1

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

Concepts Used:

- $Sym(G) := Aut_{Set}(G, G)$ is the group of set morphisms from G to itself, i.e. permutations of elements of G.
- More standard terminology: this is related to the **left regular representation** where $g \mapsto \varphi_g$ where $\varphi_g(x) = gx$, regarded instead as a permutation representation.

- This action is transitive!

• Cayley's theorem: every G is isomorphic to a subgroup of a permutation group. In particular, take $\{\varphi_g \mid G \in G\}$ with function composition as a subgroup of $\operatorname{Aut}_{\mathsf{Set}}(G)$.

Solution:

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

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

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

- So there are m orbits all of length exactly k. Proceed by casework.
- If k is even:
 - This yields m odd cycles, and thus π has zero (an even number) of even cycles.
 - Thus $\pi \in \ker \operatorname{sgn}$ and is an even permutation.
- If k is odd
 - This yields m even cycles, thus an even number of even cycles iff m is even
- The claim is that the number of orbit representatives m is equal to $[G:H] = \sharp G/H$ for $H = \langle g \rangle$.

Proof: define a map

{Orbit representatives
$$x_i$$
} $\rightarrow G/H$
 $x \mapsto xH$.

- This is injective and surjective because

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

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

• We now have

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

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

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

• Then just recall that
$$k \coloneqq o(\pi_g)$$
 and

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

2.4.2 Fall 2015 #1

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

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

- Let $H \leq G$ and define $n \coloneqq [G:H]$.
- Write $G/H = \{x_1H, \dots, x_nH\}$ for the finitely many cosets.
- Let G act on G/H by left translation, so $g \cdot xH \coloneqq gxH$.. Call the action $\psi : G \to \text{Sym}(G/H)$.
- Then Stab $(xH) = xHx^{-1}$ is a subgroup conjugate to H, and $K \coloneqq \ker \psi = \bigcap_{i=1}^n xHx^{-1}$

is the intersection of all conjugates of H.

- Kernels are normal, so $K \leq G$, and $K \subseteq xHx^{-1}$ for all x, meaning K is contained in every conjugate of H.
- The index [G:K] is finite since $G/K \cong \operatorname{im} \psi$ by the first isomorphism theorem, and $\sharp \operatorname{im} \psi \leq \sharp \operatorname{Sym}(G/H) = \sharp S_n = n! < \infty$.

2.5 Conjugacy Classes

2.5.1 Spring 2021 #2

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

Solution due to Swaroop Hegde, typed up + modifica-tions added by DZG.

Concepts Used:

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

Strategy:

Show an element x is central by showing $\sharp C_x = 1$.

Proof (?).

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

 $H = \coprod_{i < k} C_{i_i}.$

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

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

• Take cardinality in the above equation

$$p = 1 + \sum_{\substack{j \le k \\ j \ne 1}} \sharp C_{i_j}.$$

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

•
$$\cup C_{i_i} = H$$
, so $H \subseteq Z(G)$.

2.5.2 Spring 2015 #1

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

Concepts Used:

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

Solution:

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

• Take cardinalities:

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

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

2.6 Unsorted / Counting Arguments

2.6.1 Fall 2021 #2

Give generators and relations for the non-commutative group G of order 63 containing an element of order 9.

- Idea: take a semidirect product involving C_9 and C_7 . We'll need some facts: Hom $(C_m, C_n) \cong C_d$ where $d = \gcd(m, n)$, and Aut $(C_m) \cong C_m^{\times}$ which has order $\varphi(m)$ (since one needs to send generators to generators), which can be explicitly calculated based on the prime factorization of m.
- Some calculations we'll need:
 - Aut $(C_9) \cong C_9^{\times} \cong C_{\varphi(9)} \cong C_6$, using that $\varphi(p^k) = p^{k-1}(p-1)$. - Aut $(C_7) \cong C_7^{\times} \cong C_{\varphi(7)} \cong C_6$ using that $\varphi(p) = p - 1$.
- To get a nonabelian group, we need a nontrivial semidirect product, so look at Hom(G, Aut(H)) in the two possible combinations.
 - Hom $(C_7, \operatorname{Aut}(C_9)) \cong$ Hom $(C_7, C_6) \cong C_1 := \{e\}$ using that Hom $(C_m, C_n) \cong C_d$ for $d = \operatorname{gcd}(m, n)$. So there are no nontrivial homs here, so only the direct product is possible.
 - Hom $(C_9, \operatorname{Aut}(C_7)) \cong$ Hom $(C_9, C_6) \cong C_3$, so use this!
 - Note that we don't have to consider possibilities for $C_3 \times C_3$, since including this as a factor would yield no elements of order 9.
- So take $G := C_7 \rtimes_{\psi} C_9$ for some $\psi: C_9 \to \operatorname{Aut}(C_7)$, and we can take the presentation

$$G = \left\langle x, y \mid x^7, y^9, yxy^{-1} = \psi(x) \right\rangle.$$

- It now suffices to find a nontrivial $\psi : C_7 \to C_7$. Writing it multiplicatively as $C_7 = \langle x \mid x^7 \rangle$, any map that sends x to a generator will do. It suffices to choose any k coprime to 7, and then take $\psi(x) \coloneqq x^k$, which will be another generator.
- So take

$$G = \left\langle x, y \mid x^7, y^9, yxy^{-1} = x^2 \right\rangle.$$

2.6.2 Fall 2019 Midterm #5

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

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

Concepts Used:

Important notations and definitions:

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

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

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

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

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

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

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

Theorems to remember and know how to prove:

- G/Z(G) Theorem: If G/Z(G) is cyclic, then G is abelian, i.e., G/Z(G) is in fact trivial.
- Lagrange's Theorem: If G is a group of finite order and H is a subgroup of G, then the order of H divides that of G.
 - One consequence of this is that every group of prime order is cyclic.

- A p-group (a group of order p^n for some prime p and some positive integer n) has nontrivial center.
- A consequence of the theorems above: every group of order p^2 (where p is prime) is abelian.

Solution:

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

2.6.3 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.

Concepts Used:

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

Strategy:

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

Proof (of a).

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

Proof (of b).

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

$$\begin{split} \psi(y)h &= \psi(y)(\psi \circ \psi^{-1})(h) \\ &= \psi(y \cdot \psi^{-1}(h)) \\ &= \psi(\psi^{-1}(h) \cdot y) \\ &= h\psi(y). \end{split}$$

since $\psi^{-1}(h) \in H, y \in Z(H)$

- That $A \operatorname{ch} B \trianglelefteq C \implies A \trianglelefteq C$:
 - $A \operatorname{ch} B$ iff A is fixed by every $\psi \in \operatorname{Aut}(B)$., WTS $cAc^{-1} = A$ for all $c \in C$.
 - Since $B \leq C$, the automorphism $\psi(-) \coloneqq c(-)c^{-1}$ descends to an element of $\operatorname{Aut}(B)$.
 - Then $\psi(A) = A$ since $A \operatorname{ch} B$, so $cAc^{-1} = A$ and $A \leq C$.

2.6.4 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

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

Solution:

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

- Since $(ab)b = ab^2 = a$, we have $\langle ab, b \rangle \subseteq \langle a, b \rangle$, so $\langle ab, b \rangle = \langle a, b \rangle$.
- Write $D_{2n} = F(r,s) / \ker \pi$ for $\pi : F(r,s) \to D_{2n}$ the canonical presentation map.
- Define

$$\psi: F(r,s) \to G$$
$$r \mapsto ab$$
$$t \mapsto b.$$

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

 $(ab)^n = e$ by construction, $b^2 = e$ by assumption, and

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

corresponding to the relation $srs^{-1} = r^{-1}$. Here we've used that o(a) = o(b) = 2 implies $a = a^{-1}, b = b^{-1}$.

- Surjectivity of $\tilde{\psi}$ yields $2n = \sharp D_{2n} \ge \sharp G$.
- The claim is that $\sharp G \geq 2n$, which forces $\sharp G = 2n$. Then $\tilde{\psi}$ will be a surjective group morphism between groups of the same order, and thus an isomorphism.
 - We have $\langle ab \rangle \leq G$, so $n \mid \sharp G$.
 - Since $b \notin \langle ab \rangle$, this forces $\sharp G > n$, so $\sharp G \ge 2n$.

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

2.6.5 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. :::

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

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

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

- If $n_p = 1$ or $n_q = 1$, we're done, so suppose otherwise.
- Case 1: : p > q.
 - Using that $[n_p]_p \equiv 1$, consider reducing elements in $\{1, q\} \mod p$.
 - Since q < p, we just have $q \mod p = q$, and as long as $q \neq 1$ we have $q \not\equiv 1 \mod p$. But since $n_p \neq 1$ and $n_p \neq q$, this is a contradiction.
- Case 2: *p* < *q*:
 - Using that $[n_q]_q \equiv 1$, consider reducing $\{1, p, p^2\} \mod q$.
 - Since now p < q, we have $p \mod q = p$ itself, so $p \mod q \neq 1$ and we can rule it out.
 - The remaining possibility is $n_q = p^2$.
 - Supposing that $n_p \neq 1$, we have $n_p = q$, so we can count

Elements from Sylow
$$q: n_q(\sharp S_q - 1) = p^2(q-1) + 1$$
,

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

- Suppose all Sylow *ps* intersect trivially, we get at least

Elements from Sylow
$$p: n_p(\sharp S_p - 1) = q(p^2 - 1).$$

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

$$q(p^{2}-1) + p^{2}(q-1) + 1 = p^{2}q - q + p^{2}q - p^{2} + 1 = p^{2}q + (p^{2}-1)(q-1) > p^{2}q = \sharp G,$$

provided $(p^2-1)(q-1) \neq 0$, which is fine for $p \geq 2$ since this is at least $(2^2-1)(3-2) = 3$ (since p < q and q = 3 is the next smallest prime).

- Otherwise, we get two Sylow ps intersecting nontrivially, which must be in a subgroup of order at least p since the intersection is a subgroup of both. In this case, just considering these two subgroups, we get

Elements from Sylow $p: n_p(\sharp S_p - 1) > p^2 + p^2 - p = 2p^2 - p - 1.$

Then a count:

$$p^{2}(q-1) + (2p^{2} - p - 1) + 1 = p^{2}q - p^{2} + 2p^{2} - p$$
$$= p^{2}q + p^{2} - p$$
$$= p^{2}q + p(p-1)$$
$$> p^{2}q = \sharp G,$$

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

2.6.6 Fall 2019 Midterm #4

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

3 Groups: Group Actions

3.1 Fall 2012 #1

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

- a. Let $x \in X$ and $G_x := \{g \in G \mid g \cdot x = x\}$. Show that G_x is a subgroup of G.
- b. Let $x \in X$ and $G \cdot x := \{g \cdot x \mid g \in G\}$. 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.

 \sim

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

~

Solution:

Proof (of a).

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

$$\begin{split} h \in \operatorname{Stab}(x) & \Longleftrightarrow h \cdot x = x \\ & \Longleftrightarrow h \cdot (g^{-1} \cdot y) = g^{-1} \cdot y \\ & \Leftrightarrow (ghg^{-1}) \cdot y = y \\ & \Leftrightarrow ghg^{-1} \in G_y \\ & \Leftrightarrow h \in g^{-1}\operatorname{Stab}(y)g, \end{split}$$

by being in the stabilizer

by definition

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

Proof (of b).

Let G act on its subgroups by conjugation,

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

ī

• 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

ı.

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

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

$$\left| \bigcup_{g \in G} g H g^{-1} \right| < (\text{Number of Conjugates of } H) \cdot (\text{Size of each conjugate})$$

strictly overcounts since they intersect in at least the identity $= [G: N_G(H)]|H|$

$$= \frac{|G|}{|N_G(H)|} |H|$$

since *G* is finite

$$\leq \frac{|G|}{|H|}|H$$
$$= |G|.$$

Proof (of c).

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

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

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

4 Groups: Sylow Theory

4.1 Fall 2019 #1

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

Concepts Used:

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

Solution:

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

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

$$g \in G \implies g = hg_j h^{-1} \qquad \text{for some } h \in H$$
$$g_j \in Z(g_k) \forall k \implies g \in hZ(g_k) h^{-1} \qquad \text{for some } h, \forall 1 \le k \le n$$
$$\implies g \in \bigcup_{h \in G} hZ(g_k) h^{-1} \qquad \forall 1 \le k \le n$$

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

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

and we're done.

4.2 Fall 2019 Midterm #2

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

4.3 Fall 2013 #2

Let G be a group of order 30.

- a. Show that G has a subgroup of order 15.
- b. Show that every group of order 15 is cyclic.
- c. Show that G is isomorphic to some semidirect product $\mathbf{Z}_{15} \rtimes \mathbf{Z}_2$.
- 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).

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 $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$ by exhibiting an appropriate set of cycles.
- b. Show that H is normal in G.
- c. Give generators and relations for G as an abstract group, such that all generators have order 3. Also exhibit elements of S_9 in cycle notation corresponding to these generators.
- d. Without appealing to the previous parts of the problem, show that G contains an element of order 9.

4.5 Fall 2014 #2

Let G be a group of order 96.

- a. Show that G has either one or three 2-Sylow subgroups.
- b. Show that either G has a normal subgroup of order 32, or a normal subgroup of order 16.

4.6	Spr	ing	201	6 :	#3
					<i></i>

- a. State the three Sylow theorems.
- b. Prove that any group of order 1225 is abelian.
- c. Write down exactly one representative in each isomorphism class of abelian groups of order 1225.

4.7 Spring 2017 #2

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

- b. Prove that if G is a group of order 56, then either the Sylow-2 subgroup or the Sylow-7 subgroup is normal.
- c. Give two non-isomorphic groups of order 56 where the Sylow-7 subgroup is normal and the Sylow-2 subgroup is *not* normal. Justify that these two groups are not isomorphic.

4.8 Fall 2017 #2

Problem 4.8.1 (?)

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.

Concepts Used:

- Classifying abelian groups of order n: factor $n = \prod_{i=1}^{k} p_i^{n_i}$, then there are $p(n_1)p(n_2)\cdots p(n_k)$ abelian groups of that order, where $p(\ell)$ is the integer partition function.
- Transitive subgroups of S_n :

 - $\begin{array}{l} -n = 3 \rightsquigarrow S_3, A_3 \\ -n = 4 \rightsquigarrow S_4, A_4, D_4, C_4, C_2^2 \text{ where } C_n \text{ is a cyclic group.} \\ -n = 5 \rightsquigarrow S_5, A_5, F_{20}, D_{10}, C_5. \end{array}$
- Background for this question: there is a theorem that if $\sharp G = p^2 q^2$ with p < q then G must have a normal q-Sylow subgroup unless $\sharp G = 36$, the only counterexample, in which case G has *either* a normal Sylow 2-subgroup or a normal Sylow 3-subgroup. The counterexample is evidenced by $C_3 \times A_4$, which has $n_3 = 4$.
 - The reason this happens: p = 2, q = 3 are consecutive primes!

Warning 4.8.1

This is slightly more difficult/lengthy than the average group theory problem in recent years.

Solution:

Part a: write $36 = 2^2 \cdot 3^2$, then the distinct groups correspond to all combinations of integer partitions of the exponents 2 and 2:

- $(2,2) \rightsquigarrow (\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/9\mathbf{Z})$
- $(1+1,2) \rightsquigarrow (\mathbf{Z}/2\mathbf{Z})^2 \times (\mathbf{Z}/9\mathbf{Z})$
- $(2,1+1) \rightsquigarrow \mathbf{Z}/4\mathbf{Z} \times (\mathbf{Z}/3\mathbf{Z})^2$
- $(1+1,1+1) \rightsquigarrow (\mathbf{Z}/2\mathbf{Z})^2 \times (\mathbf{Z}/3\mathbf{Z})^2$

Part b: let $H_2 \leq G$ be the unique Sylow 2-subgroup, so $\sharp H_2 = 2^2$. Then $H_2 \leq G$, so G/H is a group of size $[G : H] = 3^2$. Note that by pure numeric observation (and the hint), it is necessary to find a normal subgroup $N \leq G$ of size 3 and thus index 12, since $\sharp A_4 = 4!/2 = 12 = 36/3$. Since normal subgroups are kernels of homomorphisms, we can look for a morphism $\varphi : G \to S_4$ where ker(φ) is order 3, anticipating applying the first isomorphism theorem to get $G/\ker(\varphi) \cong \operatorname{im}(\varphi) \leq S_4$, where we hope that $\operatorname{im}(\varphi) \cong A_4$. So we look for an action of G on a set with 4 elements.

Applying the Sylow theorems, we have $n_3 \mid 2^2 \implies n_3 \in \{1, 2, 4\}$ and $n_3 \equiv 1 \mod 4 \implies n_3 \in \{1, 4\}$. Note that $n_3 = 1$ implies the Sylow 3-subgroup is normal, in which case $G \cong H_2 \times H_3$ splits into a product of groups of order $2^2, 3^2$, and thus G is abelian since any group of order p^2 is abelian for any prime p and products of abelian groups are abelian. So we can conclude that $n_3 = 4$ and consider the action of G on the set of four Sylow 3-subgroups of G to get a map $\varphi: G \to S_4$.

It is a theorem that this action is transitive, and so $\operatorname{im}(\varphi)$ is a transitive subgroup of S_4 . By standard facts in Galois theory, the only such subgroups are $S_4, A_4, D_4, C_2^2, C_4$, and so $\#\operatorname{im}(\varphi) \in \{24, 12, 8, 4\}$. By the hint it suffices to show that $\#\operatorname{im}(\varphi) = 12$.

- $\sharp \operatorname{im}(\varphi) \neq 24$, since then φ surjects and $G/\ker(\varphi) \cong S_4$, but the RHS has order 24 and the LHS order 36/k for some $k \in \mathbb{Z}$, which is impossible.
- $\sharp \operatorname{im}(\varphi) \neq 8$ since then 36/k = 8 for some k, again impossible.
- $\# \operatorname{im}(\varphi) \neq 4$: if so, $\# \operatorname{ker}(\varphi) = 9$ so $\operatorname{ker}(\varphi)$ is a Sylow 3-subgroup. Since kernels are normal and all Sylows are conjugate, this would force $n_3 = 1$, a contradiction.

Summarizing, to produce N, consider $G \curvearrowright \text{Syl}_3(G)$ to get a map $\varphi : G \to S_4$. Then $\text{im}(\varphi) \leq S_4$ must have order 12 with kernel $N \coloneqq \text{ker}(\varphi)$ of order 3, and since the only subgroup of order 12 in S_4 is A_4 , we have $G/N \cong A_4$.

Part 3: Since $N \leq G$, we need to show:

- $H \cap N = \{e\},$
- NH = G,
- $H \trianglelefteq G$

The first two conditions will give a semidirect product, and the third will show that the semidirect product is actually direct.

Note that $L := H \cap N$ is a subgroup of both H and N, so if $L \neq \{e\}$ then $\sharp L = 3$ and L is a subgroup of both N and A_4 . So L = N and thus $N \subseteq A_4$ is a cyclic subgroup of order 3 generated by (say) n; however since $2 \mid \sharp A_4 = 12$, Cauchy's theorem produces an element mof order two. But then the subgroup $\langle n, m \rangle$ is an order 6 subgroup of A_4 , which by the hint does not exist, so by contradiction we must have $L := N \cap H = \{e\}$. That NH = G now follows by counting elements: $NH \leq G$ is a subgroup, and $\sharp NH = (\sharp N) \cdot (\sharp H) = 3 \cdot 12 = \sharp G$.

Finally, to see that $H \leq G$, we'll instead show that the semidirect product is trivial directly. By the first two conditions above, we already have $G \cong N \rtimes_{\varphi} H$ for some $\varphi : H \to \operatorname{Aut}(N)$. Since $N \cong C_3$ is cyclic, $\operatorname{Aut}(N) \cong N^{\times}$ which is of order $\varphi(3) = 2$, so φ is a group morphism from a group of order 12 to one of order 2. If φ is nontrivial, $\sharp \ker \varphi = 12/2 = 6$ is a subgroup of order 6 in $H \cong A_4$, contradicting the hint and forcing φ to be trivial and $G \cong H \times N$. **Part d** If $G \coloneqq D_{18}$ has a normal Sylow 2-subgroup, by part $2 \exists N \leq G$ with $G/N \cong A_4$, and (claim) since G has a subgroup $H \cong A_4$ we must have $G = N \times H$, a product of groups of orders 3 and 12 respectively. Somehow this is a contradiction??

That $H \cong A_4 \leq G$ exists: unclear, maybe even not true. Not sure what the intended approach is, so here's an alternative.

A general fact: for D_{2n} , for any odd prime $p \mid 2n$, the Sylow *p*-subgroup H_p is cyclic and normal since $D_{2n} \cong C_n \rtimes C_2$ and p > 2 implies H_p descends to a Sylow *p*-subgroup of C_n and all subgroups of cyclic groups are abelian and cyclic. Here n = 18, so take p = 3 to get $H_3 \leq D_{18}$ a normal subgroup of order 9. If $n_2 = 1$, so there is one single normal Sylow 2-subgroup, then H_2, H_3 are both normal and we get $D_{18} \cong H_2 \times H_3$ as a direct product. But H_2, H_3 are abelian and D_{18} is nonabelian, so this is a contradiction.

4.9 Fall 2012 #2

Let G be a group of order 30.

- a. Show that G contains normal subgroups of orders 3, 5, and 15.
- b. Give all possible presentations and relations for G.
- c. Determine how many groups of order 30 there are up to isomorphism.

4.10 Fall 2018 #1

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

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



Concepts Used:

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

Solution:

Proof (of a).

- Every p-subgroup is contained in some Sylow p-subgroup, so $P \subseteq S_p^i$ for some $S_p^i \in \text{Syl}_p(G)$.
- $P \trianglelefteq G \iff gPg^{-1} = P$ for all $g \in G$.
- Let S_p^j be any other Sylow *p*-subgroup,
- Since Sylow *p*-subgroups are all conjugate $gS_p^ig^{-1} = S_p^j$ 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
$$a \le c \implies 0 \le c - b \le c$$
 so $0 \le b \le c$.

4.11 Fall 2019 #2

```
4.10 Fall 2018 #1
```

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

- a. Prove that at least one of Q and R is normal in G.
- b. Prove that G has a cyclic subgroup of order 35.
- c. Prove that both Q and R are normal in G.
- d. Prove that if P is normal in G then G is cyclic.

Concepts Used:

- The pqr theorem.
- Sylow 3: $|G| = p^n m$ implies $n_p \mid m$ and $n_p \cong 1 \mod p$.
- **Theorem**: If $H, K \leq G$ and any of the following conditions hold, HK is a subgroup:
 - $H \trianglelefteq G \text{ (wlog)}$ - [H, K] = 1 $- H \le N_G(K)$
- **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, $q 1 \neq 0 \mod p$.
- Theorem:

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

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

Solution:

4

Proof (of 1).

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

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

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

 $|Syl(5) \cup Syl(7)| = (5-1)n_5 + (7-1)n_7 + 1 = 4(21) + 6(15) = 174 > 105$ 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 $Q, R \leq G$, so we proceed by showing **not** $(n_5 = 21 \text{ or } n_7 = 15)$, which is equivalent to $(n_5 = 1 \text{ and } n_7 = 1)$ by the previous restrictions.
- Note that we can write

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

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

- Elements in QR of order **not** equal to 5: $|QR Q\{id\} + \{id\}| = 35-5+1 = 31$ - Elements in QR of order **not** equal to 7: $|QR - \{id\}R + \{id\}| = 35-7+1 = 29$
- Since $QR \leq G$, we have
 - Elements in G of order **not** equal to $5 \ge 31$.
 - Elements in G of order **not** equal to $7 \ge 29$.
- Now both cases lead to contradictions:
 - $-n_5=21:$

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

 $-n_7 = 15:$

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

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

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

by the Chinese Remainder Theorem, which is cyclic.

- a. Show that every group of order p^2 with p prime is abelian.
- b. State the 3 Sylow theorems.
- c. Show that any group of order $4225 = 5^2 13^2$ is abelian.
- d. Write down one representative from each isomorphism class of abelian groups of order 4225.

4.13 Fall 2020 #1

- a. Using Sylow theory, show that every group of order 2p where p is prime is not simple.
- b. Classify all groups of order 2p and justify your answer. For the nonabelian group(s), give a presentation by generators and relations.

4.14 Fall 2020 #2

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

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

5 | Groups: Classification

5.1 Spring 2020 #1

- a. Show that any group of order 2020 is solvable.
- b. Give (without proof) a classification of all abelian groups of order 2020.
- c. Describe one nonabelian group of order 2020.

Work this problem.

5.2 Spring 2019 #3

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

Describe a representative from each class.

Concepts Used:

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

Solution:

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

Revisit, seems short.

5.3 Spring 2012 #3

Let G be a group of order 70.

- a. Show that G is not simple.
- b. Exhibit 3 nonisomorphic groups of order 70 and prove that they are not isomorphic.

5.4 Fall 2016 #3

5.2 Spring 2019 #3

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

5.5 Spring 2018 #1

- a. Use the Class Equation (equivalently, the conjugation action of a group on itself) to prove that any p-group (a group whose order is a positive power of a prime integer p) has a nontrivial center.
- b. Prove that any group of order p^2 (where p is prime) is abelian.
- c. Prove that any group of order $5^2 \cdot 7^2$ is abelian.
- d. Write down exactly one representative in each isomorphism class of groups of order $5^2 \cdot 7^2$.

Concepts Used:

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

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

- 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

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

- Thus every index appearing in the sum is greater than 1, and thus equal to p^{ℓ_i} for some $1 \le \ell_i \le k$
- 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 $|Z(G)| \ge p$.

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

 $\begin{array}{ll} -n_5 \mid 7^2, & n_5 \cong 1 \mod 5 \implies n_5 \in \{1, 7, 49\} \setminus \{7, 49\} = \{1\} \implies n_5 = 1 \\ -n_7 \mid 5^2, & n_7 \cong 1 \mod 7 \implies n_7 \in \{1, 5, 25\} \setminus \{5, 25\} = \{1\} \implies n_7 = 1 \end{array}$

- By recognition of direct products, $G = S_5 \times S_7$
 - By above, $S_5, S_7 \leq G$
 - Check $S_5 \cap S_7 = \{e\}$ since they have coprime order.
 - Check $S_5S_7 = G$ since $|S_5S_7| = 5^27^2 = |G|$
- 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).

•
$$\mathbf{Z}_{5^2} imes \mathbf{Z}_{7^2}$$

- $\mathbf{Z}_{5}^{2} \times \mathbf{Z}_{7^{2}}$ $\mathbf{Z}_{5^{2}} \times \mathbf{Z}_{7}^{2}$ $\mathbf{Z}_{5^{2}} \times \mathbf{Z}_{7}^{2}$ $\mathbf{Z}_{5}^{2} \times \mathbf{Z}_{7}^{2}$

Groups: Simple and Solvable h

6.1 * Fall 2016 #7

- a. Define what it means for a group G to be *solvable*.
- b. Show that every group G of order 36 is solvable.

Hint: you can use that S_4 *is solvable.*

6.2 Spring 2015 #4

Problem 6.2.1 (?) Let N be a positive integer, and let G be a finite group of order N.

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

$$C: G \to \operatorname{Sym}^* G$$
$$g \mapsto (x \mapsto gx)$$

is an injective homomorphism.

- b. Let Φ : 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 $N \equiv 2 \mod 4$. Prove that G is not simple.

Hint: use part (b).

Warning 6.2.1

We haven't *really* covered the Cayley representation ("left-regular representation") in the qual class in recent years, and this question uses some slightly nontrivial properties of it.

Concepts Used:

- A cycle $\sigma \in S_N$ is odd $\iff \varepsilon(\sigma) = -1 \iff \sigma$ has an odd number of even cycles $\iff \sigma$ can be written as an even number of transpositions.
- A single cycle of even length is odd, and of odd length is even, by writing $(123\cdots, d) = (12)(13)\cdots(1d)$, reading right-to-left.
- $A_n := \ker(S_n \to \mathbb{Z}/2\mathbb{Z})$ is the kernel of the sign morphism, so only even permutations.

Solution:

Part a: Check that ker $C = \{e\} \subseteq G$, or prove injectivity directly via $C(g) = C(h) \implies g = h$. For the former, introduce some new notation: write

$$C: G \to \operatorname{Sym}(G)$$
$$g \mapsto \tau_g.$$

where

$$\tau_g: G \to G$$
$$x \mapsto gx$$

is left-translation by g. Now note that the identity in Sym(G) is the group morphism id_G , so

$$\ker(C) \coloneqq \left\{ g \in G \mid C(g) = \mathrm{id}_G \right\}$$
$$= \left\{ g \in G \mid \tau_g(x) = x \ \forall x \in G \right\}$$
$$= \left\{ g \in G \mid gx = x \ \forall x \in G \right\}$$
$$= \bigcap_{x \in G} \mathrm{Stab}_G(x),$$

i.e. anything in the kernel is (by definition) in the stabilizer of every point $x \in G$. Now check that

 $g \in \operatorname{Stab}_G(x) \iff gx = x \iff gxx^{-1} = xx^{-1} \iff ge = e \iff g = e$

where e is the identity in G, so $\operatorname{Stab}_G(x) = \{e\}$ for every $x \in G$ and thus $\ker(C) = \{e\}$.

Note: one should also prove that C is actually a

group morphism, but this is mostly a routine check. **Part b:** Let $\Psi : G \to S_N$ be the composition $\Psi = \Phi \circ C$; this is a group morphism and ker $\Psi \trianglelefteq G$ is always a normal subgroup (which is used in part c).

Fix $a \in G$ with d defined as the order of a.

 \Leftarrow : Suppose *d* is even and *N*/*d* is odd. Let $A \coloneqq \langle a \rangle$, then [G : H] = N/d, so there are an odd number of (left) *A*-cosets. Consider the permutation $\Psi(a) \in S_N$; the claim is that τ_a is a product of *N*/*d* cycles, all of length *d*. Given this claim, under our assumptions $\Psi(a)$ has an **odd number of even cycles**, is thus an odd permutation, and thus $\varepsilon(a) = -1$.

 \implies : Suppose $\varepsilon(a) = -1$, then $\Psi(a)$ is an odd permutation. Since $\Psi(a)$ is in the image of Ψ , it can be written as a product (not necessarily unique) of N/d cycles of length d. Since this cycle must be odd, there must be an odd number of even cycles in any such decomposition. One can show that all cycles in the image of the left-regular representation are the same length, so every cycle is of even length d, and there are an odd number N/d of them.

Part c: . Since a sufficient condition for G not to be simple is existence of a nontrivial normal subgroup, it suffices to cook up a nontrivial $a \in \ker \Psi$. Note that

 $N \equiv 2 \mod 4 \implies 2 \mid N \text{ and } 2^2 \nmid N \implies N/2 \text{ is odd},$

so with the hint in mind, consider $d \coloneqq 2$. Suppose

$$\ker(\Psi) \coloneqq \left\{ a \in G \mid \varepsilon(a) = 1 \right\} = \left\{ e \right\},\$$

then this forces $\varepsilon(a) = -1$ for every nontrivial $a \in G$. Letting d(a) be the order of a, we know that d(a) must be even and N/d(a) must be odd for every a. Since d(a) is even, $2 \mid d(a)$, but since $2^2 \mid N$, we must have $2^2 \mid d(a)$. So d(a) is an even number (so no odd prime factors) with exactly one copy of 2 in its prime factorization, forcing d(a) = 2 for all $a \in G$.

But now every element in G is order 2, and a one can show the general result that if every $g \in G$ satisfies $g^2 = e$ then the size of G is a power of 2. However, since N/2 is necessarily odd, this is a contradiction. f

So there must be some $a \in G$ with $\varepsilon(a) = 1$, making ker $(\Psi) \leq G$ nontrivial and exhibiting a normal subgroup that makes G non-simple.

For the power of 2 result, one can use Cauchy's theorem: if any odd prime $p \ge 3$ divides the size of G, then there exists an element of order p, contradiction.

6.3 Spring 2014 #1

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

6.4 Fall 2013 #1

Let p, q be distinct primes.

- a. Let $\overline{q} \in \mathbf{Z}_p$ be the class of $q \mod p$ and let k denote the order of \overline{q} as an element of \mathbf{Z}_p^{\times} . Prove that no group of order pq^k is simple.
- b. Let G be a group of order pq, and prove that G is not simple.

6.5 Spring 2013 #4

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

6.6 Fall 2019 Midterm #3

Show that there exist no simple groups of order 148.

7 | Commutative Algebra

7.1 UFDs, PIDs, etc

7.1.1 Spring 2013 #2

- a. Define a Euclidean domain.
- b. Define a *unique factorization domain*.
- c. Is a Euclidean domain an UFD? Give either a proof or a counterexample with justification.
- d. Is a UFD a Euclidean domain? Give either a proof or a counterexample with justification.

Solution:

- R is Euclidean iff it admits a Euclidean algorithm: there is a degree function $f : R \to \mathbb{Z}_{\geq 0}$ such that for all $a, b \in R$, there exist $q, r \in R$ such that a = bq + r where f(r) < f(b) or r = 0.
- *R* is a UFD iff every $r \in R$ can be written as $r = u \prod_{i=1}^{n} p_i$ with $n \ge 0$, $u \in R^{\times}$, and p_i irreducible. This is unique up to associates of the p_i and reordering.
- Euclidean implies UFD:
 - Euclidean implies PID:
 - ♦ If $I \in Id(R)$ one can use the degree function to find any $b \in I$ where f(b) is minimal.
 - ♦ Then $I = \langle b \rangle$, since if $a \in I$ one can write a = bq + r and use that $a bq \in I \implies r \in I$.
 - \diamond But by minimality, we can't have f(r) < f(b), so r = 0 and $a \mid b$, so $b \in \langle a \rangle$.
 - PID implies UFD:
 - \diamond Use that irreducible implies prime in a PID, so every $x \in R$ has some factorization into finitely many primes.
 - ♦ Supposing $x = u_p \prod_{i=1}^m p_i = u_q \prod_{i=1}^n q_i$, use that p_1 divides the LHS and so p_1 divides the RHS. WLOG, $p_1 | q_1$, so $q_1 = u_1 p_1$ for $u \in \mathbb{R}^{\times}$, so $x = u_q u_1 p_1 \prod_{i=2}^m q_i$ by rewriting a term on the RHS.
 - \diamond Note that this makes p_1, q_1 associates.

 \diamond Continuing up to m, we get

$$x = u_p \prod_{i=1}^m p_i$$

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

where we've moved all units to the LHS. This makes p_i, q_i associates for $i \leq m$. \diamond But primes aren't units and the product of nontrivial primes can't be a unit,

- so the right-hand side product must be empty.
- \diamond So m = n and all p_i, q_i are associate, QED.
- UFD does not imply Euclidean:
 - It suffices to find a UFD that is not a PID.
 - Take $R := \mathbf{C}[x, y]$, which is a UFD by the usual factorization of polynomials. It is not a PID, since $\langle 2, x \rangle$ is not principal.

7.1.2 Fall 2017 #6

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

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

- a. Prove R is an integral domain.
- b. Show $U(R) = \{\pm 1\}.$
- c. Show $3, 2 + \sqrt{-5}$, and $2 \sqrt{-5}$ are irreducible in R.
- d. Show 3 is not prime in R.
- e. Conclude R is not a PID.

Concepts Used:

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

Solution:

- *R* is an integral domain:
 - Let $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$ and set $\overline{\alpha}, \overline{\beta}$ be their conjugates. - Then

$$0 = \alpha\beta = \alpha\overline{\alpha}\beta\overline{\beta} = (a^2 - 5b^2)(c^2 - 5d^2) \in \mathbf{Z},$$

so one factor is zero.

- If $a^2 = 5b^2$ then $a = \sqrt{5}b \notin \mathbb{Z}$ unless a = b = 0. Otherwise, the same argument forces c = d = 0.
- The units are ± 1 :
 - Use that $u \in \mathbb{R}^{\times} \implies N(u) = \pm 1$, and $N(\alpha) = \alpha \overline{\alpha} = (a + b\sqrt{-5})(a b\sqrt{-5}) = a^2 + 5b^2 = 1$ forces b = 0 and $a = \pm 1$.
- Irreducible elements:
 - 2,3 are irreducible because if (say) 3 = xy then N(x)N(y) = N(3) = 9, and if neither x, y are units then N(x) = N(y) = 3. But $N(a + b\sqrt{-5}) = a^2 + 5b^2$ and $a^2 + 5b^2 = 3$ has no solutions. The same argument works for 2.
 - $-2 \pm \sqrt{-5}$ are irreducible because $N(2 + \sqrt{-5}) = 2^2 + 5(1) = 9$, and in fact $N(2 \sqrt{-5}) = 2^2 + 5(-1)^2 = 9$. By the same argument as above, this forces irreducibility.
- 3 is not prime:
 - We can write $6 = (3)(2) = (1 + \sqrt{-5})(1 \sqrt{-5})$, so if we assume 3 is prime we get $3 \mid (1 \pm \sqrt{-5})$.
 - But writing $(1 \pm \sqrt{-5}) = 3r$ for some $r \in R$ yields

$$(1 \pm \sqrt{-5}) = 3(a + b\sqrt{-5}) \implies 3a = 1, 3b = \pm 1.$$

These have no solutions $a, b \in \mathbb{Z}$.

- R is not a PID:
 - Use that irreducibles are prime in a UFD, which is not true here.

7.1.3 Spring 2017 #4

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

Prove that R is not a UFD.

(You may assume Gauss' lemma)

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

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

Concepts Used:

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

Solution:

Proof (of 1).

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

Proof (of b).

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

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

7.2.1 Fall 2021 #5 #algebra/qual/stuck

Let R be an algebra over \mathbb{C} which is finite-dimensional as a \mathbb{C} -vector space. Recall that an ideal I of R can be considered as a \mathbb{C} -subvector space of R. We define the codimension of I in R to be

 $\operatorname{codim}_R I \coloneqq \operatorname{dim}_{\mathbf{C}} R - \operatorname{dim}_{\mathbf{C}} I,$

the difference between the dimension of R as a C-vector space, $\dim_{\mathbf{C}} R$, and the dimension of I as a C-vector space, $\dim_{\mathbf{C}} I$.

- a. Show that any maximal ideal $m \subset R$ has codimension 1 .
- b. Suppose that $\dim_{\mathbf{C}} R = 2$. Show that there exists a surjective homomorphism of **C**-algebras from the polynomial ring $\mathbf{C}[t]$ to R.
- c. Classify such algebras R for which $\dim_{\mathbf{C}} R = 2$, and list their maximal ideals.

Solution:

Part a: Since I is proper, we have $\operatorname{codim}_R I \ge 1$ since $\operatorname{codim}_R I = 0 \implies I = R$ since $I \le R$ is a vector subspace of the same dimension. We also have $\operatorname{codim}_R I \le \dim_{\mathbb{C}} R$, and noting that $\operatorname{codim}_R I = \dim_{\mathbb{C}} R \iff \dim_{\mathbb{C}} I = \dim_{\mathbb{C}} R$ and if I is maximal it is necessarily proper, we in fact have $\operatorname{codim}_R I < \dim_{\mathbb{C}} R$, so

$$1 \leq \operatorname{codim}_{R} I \leq \dim_{\mathbf{C}} R - 1.$$

Now if $\operatorname{codim}_R I \geq 2$, then $\dim_{\mathbf{C}} I \leq \dim_{\mathbf{C}} R - 2$. Choosing a basis $\{v_1, \dots, v_n\}$ for R as a **C**-vector space induces a basis $\{v_1, \dots, v_k\}$ on I for some $k \leq n - 2$. But then $I' := \langle v_1, \dots, v_k, v_{k+1} \rangle$ is a proper **C**-vector subspace of R containing I, contradicting maximality of I. So $\operatorname{codim}_R I < 2$, forcing $\operatorname{codim}_R I = 1$.

Part b: Choose a vector space basis $\{v_1, v_2\}$ for R and define a map

$$\begin{split} \varphi: \mathbf{C}[t] &\to R \\ 1 &\mapsto v_1 \\ t &\mapsto v_2, \end{split}$$

extended by linearity.

Part c: By part (b), $R \cong \mathbb{C}[t]/I$ where $I = \ker \varphi$ (using the first isomorphism theorem). Since $\mathbb{C}[t]$ is a PID, we have $I = \langle f \rangle$ for some monic f. We must have deg $f = \dim_{\mathbb{C}} \mathbb{C}[t]/I = \dim_{\mathbb{C}} R = 2$, so f is a quadratic. Since \mathbb{C} is algebraically closed we can write $f(z) = (z-a)(z-\overline{a})$ or $f(z) = (z-a)^2$ for some $a \in \mathbb{C}$. By the ideal correspondence theorem, maximal ideals of R correspond to maximal ideals of $\mathbb{C}[t]$ containing I, and again using that $\mathbb{C}[t]$ is a PID, these correspond to ideals $\langle g \rangle$ with $g \mid f$ (to contain is to divide) for some $g \in \mathbb{C}[t]$. So the maximal ideals of R correspond to any of

- g(z) = 1
- g(z) = z a
- $g(z) = z \overline{a}$
- g(z) = f(z)

Thanks to Akash Singha Roy for this solution.

7.2.2 Fall 2013 #3

- a. Define *prime ideal*, give an example of a nontrivial ideal in the ring \mathbf{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 ${\bf Z}$ and prove that it is maximal.

Solution:

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

7.2.3 Fall 2014 #8

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

You may assume the axiom of choice.

7.2.4 Fall 2014 #7

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

Concepts Used:

• If R[x] is a PID, then R is a field (not explicitly used).

• In $P := R[x_1, \cdots, x_n]$, there are degree functions $\deg_{x_n} : P \to \mathbb{Z}_{\geq 0}$.

Solution:

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

7.2.5 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:

$$N(R) \coloneqq \left\{ x \in R \mid x^n = 0 \text{ for some } n \right\}$$
$$J(R) \coloneqq \cap_{\mathfrak{m} \in \mathrm{mSpec}} \mathfrak{m}.$$

- 7
- 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

$$S = \left\{ J \mid I \subseteq J < R \right\}$$

which is a poset under set inclusion.

Given a chain $J_1 \subseteq \cdots$, there is an upper bound $J \coloneqq \bigcup J_i$, so Zorn's lemma applies.

 $\begin{array}{l} Proof \ (of \ b, \implies).\\ \Longrightarrow :\end{array}$

- 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 $I = \langle 1 + x \rangle \leq R$. 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 $\mathfrak{m} = R$.

 $Proof \ (of \ b, \ \Leftarrow=).$

⇐

- 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

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

- 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 $x \in J(R)$.

$$\begin{split} \mathfrak{N}(R) &\subseteq J(R): \\ \bullet \text{ Use the fact } x \in \mathfrak{N}(R) \implies x^n = 0 \implies 1 + rx \text{ is a unit } \iff x \in J(R) \text{ by (b):} \\ &\sum_{k=1}^{n-1} (-x)^k = \frac{1 - (-x)^n}{1 - (-x)} = (1 + x)^{-1}. \\ J(R) &\subseteq \mathfrak{N}(R): \\ \bullet \text{ Let } x \in J(R) \setminus \mathfrak{N}(R). \\ \bullet \text{ Since } R \text{ is finite, } x^m = x \text{ for some } m > 0. \\ \bullet \text{ Without loss of generality, we can suppose } x^2 = x \text{ by replacing } x^m \text{ with } x^{2m}. \\ \bullet \text{ If } 1 - x \text{ is not a unit, then } \langle 1 - x \rangle \text{ is a nontrivial proper ideal, which by (a)} \\ \text{ is contained in some maximal ideal } \mathfrak{m}. \text{ But then } x \in \mathfrak{m} \text{ and } 1 - x \in \mathfrak{m} \implies x + (1 - x) = 1 \in \mathfrak{m}, \text{ a contradiction.} \\ \bullet \text{ So } 1 - x \text{ is a unit, so let } u = (1 - x)^{-1}. \\ \bullet \text{ Then } \\ \begin{pmatrix} (1 - x)x = x - x^2 = x - x = 0 \\ \implies u(1 - x)x = x = 0 \\ \implies x = 0. \end{pmatrix} \end{aligned}$$

7.2.6 Spring 2018 #8

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

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 $g(x) \ge 0$ 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 $Z(I) = \{x \in [0,1] \mid f(x) = 0 \text{ for all } f \in I\}$ is nonempty.
- c. Show that if I is maximal, then there exists $x_0 \in [0,1]$ such that $I = \{f \in R \mid f(x_0) = 0\}$.

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

Solution:

Proof (of a).

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

Proof (of b).

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

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

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

Proof (of c).

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

I'm not super convinced by c!

7.3 Zero Divisors and Nilpotents

7.3.1 Spring 2014 #5

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

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

Solution:

 $A \implies B$:

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

 $A \implies B$:

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

7.3.2 Spring 2021 #5

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

Solution:

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

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

 $0 = f(x)g(x) = (a_0 + \dots + a_{n-1}x^{n-1} + a_nx^n)(b_0 + \dots + b_{m-1}x^{m-1} + b_mx^m).$

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

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

7.3.3 Fall 2018 #7

Let R be a commutative ring.

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

$$r \bullet : R \to R$$
$$x \mapsto rx.$$

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 $n \ge 2$ be an integer. Show: if R has exactly n zero-divisors, then $\sharp R \le n^2$.
- 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:

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

Concepts Used:

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

Solution:

Proof (of a).

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

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

Proof (of b).

Let $\varphi_r(x) \coloneqq rx$ be the multiplication map.

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

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

so $z \in \ker \varphi_y$.

Proof (of c).

- Let $Z \coloneqq \{z_i\}_{i=1}^n$ 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

$$|K_i| \le n < \infty$$
 for each *i*.

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

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

• But then

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

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 $|R^{\times}| \geq 2$ since ± 1 are always units, we must have |R| = 4.
- Since the characteristic of a ring must divide its size, we have ch R = 2 or 4.
- Using the hint, we see that only $\mathbf{Z}/(4)$ 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 $\mathbf{Z}/(2)[t]/(t^2) = \{a + bt \mid a, b \in \mathbf{Z}/(2)\}$, and checking the multiplication table we have

		1		1+t
0	0	0	0	0
1	0	1	t	1+t,
t	0	t	0	t
1+t	0	$\begin{array}{c} 0 \\ 1 \\ t \\ 1+t \end{array}$	t	1

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 $\mathbf{Z}/(2)[t]/(t^2 + t + 1)$, we can check the bottom-right corner of the multiplication table to find

$$\begin{bmatrix} t & 1+t \\ \hline t & 1+t & 1 \\ t & 1 & t \end{bmatrix},$$

and so this ring only has one zero divisor.

• Thus the only possibilities are:

$$\begin{split} &R\cong \mathbf{Z}/(4)\\ &R\cong \mathbf{Z}/(2)[t]/(t^2) \end{split}$$

7.4 Zorn's Lemma

7.4.1 Fall 2013 #4

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

- a. Show that the collection of nilpotent elements in R forms an ideal.
- b. Show that if x is nilpotent, then x is contained in every prime ideal of R.
- c. Suppose $x \in R$ is not nilpotent and let $S = \{x^n \mid n \in \mathbb{N}\}$. There is at least on ideal of R disjoint from S, namely (0).

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

Show that I is a prime ideal.

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

7.4.2 Fall 2015 #3

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

Prove that R contains a maximal left ideal.

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

Solution:

• Define the map

$$\varphi_u : R \to R$$
$$x \mapsto xu,$$

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

• Then $K \coloneqq \ker \varphi_u \in \mathrm{Id}(R)$ is an ideal.

- K is proper otherwise, noting Ru = R, if K = R we have Ru = 0 and thus R = 0. So suppose $R \neq 0$.
- Take a poset $S := \{J \in \mathrm{Id}(R) \mid J \supseteq K, J \neq R\}$, the set of all ideals containing K, ordered by subset inclusion. Note that $K \in S$, so S is nonempty.
- Apply Zorn's lemma: let $C: C_1 \subseteq C_2 \subseteq \cdots$ be a chain (totally ordered sub-poset) in S. If C is the empty chain, K is an upper bound. Otherwise, if C is nonempty, define $\widehat{C} \coloneqq \bigcup_{i=1}^{\infty} C_i.$
 - $-\hat{C}$ is an ideal: if $a, b \in \hat{C}$, then $a \in C_i, b \in C_j$ for some i, j. But without loss of generality, using that chains are totally ordered, $C_i \subseteq C_j$, so $a, b \in C_j$ and thus $ab \in C_j$. Similarly for $x \in \widehat{C}$, $x \in C_j$ for some j, and thus $Rx \subseteq C_j$ since C_j is an
 - \hat{C} is in S: It clearly contains K, since for example $K \subseteq C_1 \subseteq \hat{C}$.
 - \Diamond That $\widehat{C} \neq R$: an ideal equals R iff it contains a unit. But if $r \in \widehat{C}$ is a unit, $r \in C_i$ for some j is a unit, making $C_i = R$.
- So by Zorn's lemma, \hat{C} contains a maximal ideal (incidentally containing K).

7.4.3 Spring 2015 #7

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

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

Prove that every such ideal J is prime.

Solution:

- Restating, take the poset $S \coloneqq \left\{ J \in \mathrm{Id}(R) \ \Big| \ J \cap S = \emptyset, I \neq R, I \subseteq J \right\}$ ordered by inclusion. Note that S is nonempty since it contains I. It suffices to produce a maximal element of S.
- Applying Zorn's lemma, let C : C₁ ⊆ C₂ ⊆ · · · be a chain and define Ĉ := ∪C_i.
 By standard arguments, Ĉ ∈ Id(R) and Ĉ ⊇ I, and it suffices to show Ĉ ∩ S = Ø and $\widehat{C} \neq R.$
- $\widehat{C} \cap S = \emptyset$:
 - By contradiction, if $x \in \widehat{C} \cap S$ then $x \in C_j$ for some j, and $x \in S$. But then $x \in C_i \cap S = \emptyset.$
- $\widehat{C} \neq R$:
 - By contradiction, if so then $1 \in \hat{C} \implies 1 \in C_j$ for some j, forcing $C_j = R$.
- So Zorn's lemma applies and we obtain some ideal **p**, which we now claim is prime.

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

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

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

7.4.4 Spring 2013 #1

Let R be a commutative ring.

- a. Define a maximal ideal and prove that R has a maximal ideal.
- b. Show than an element $r \in R$ is not invertible $\iff r$ is contained in a maximal ideal.
- c. Let M be an R-module, and recall that for $0 \neq \mu \in M$, the annihilator of μ is the set

Ann
$$(\mu) = \left\{ r \in R \mid r\mu = 0 \right\}.$$

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

Prove that I is a prime ideal.

Solution:

Proof (part a and b).

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

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

 \implies :

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

Proof (of d).

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

7.4.5 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 $\{I \leq R \mid J \cap S = \emptyset\}$ 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 $S = \left\{ r^k \mid k \in \mathbb{N} \right\}$ 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, $\{I \leq R \mid I \cap S = \emptyset\}$ has a maximal element \mathfrak{p} .
- Since R is commutative, \mathfrak{p} is prime.

Proof (of c).

- Suppose *R* has a unique prime ideal **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 ∈ p.
- Since r ∉ N, by (b) there is a maximal ideal m that avoids all positive powers of r.
 Since m is prime, we must have m = p. But then r ∉ p, a contradiction.

7.5 Noetherian Rings

7.5.1 Fall 2015 #4

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

Solution:

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

7.5.2 Spring 2021 #6

- a. Carefully state the definition of **Noetherian** for a commutative ring R.
- b. Let R be a subset of $\mathbf{Z}[x]$ consisting of all polynomials

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

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

c. Show that R is not Noetherian.

Hint: consider the ideal generated by $\left\{2x^k \mid 1 \le k \in \mathbf{Z}\right\}$.

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

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

yields an ideal that is not finitely generated.

• Suppose toward a contradiction that $\{g_1, g_2, \cdots, g_M\}$ were a finite generating set, where each $g_i \in I$.

7.6 Simple Rings

7.6.1 Fall 2017 #5

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

- a. Suppose R is a commutative ring with 1. Prove R is simple if and only if R is a field.
- b. Let k be a field. Show the ring $M_n(k)$, $n \times n$ matrices with entries in k, is a simple ring.

Concepts Used:

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

Solution: • A ring is **Noetherian** iff *R* satisfies the ascending chain condition: every chain of ideals $A_1 \subseteq A_2 \subseteq \cdots$ eventually stabilizes, so $A_m \subseteq A_{m+1} = A_{m+2} = \cdots$.

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

Solution:

Proof (of a).

 \Longrightarrow :

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

⇐ :

- Suppose R is a field and $I \in Id(R)$ is an ideal.
- If $I \neq \langle 0 \rangle$ is proper and nontrivial, then I contains at least one nonzero element $a \in I$.
- Since R is a field, $a^{-1} \in R$, and $aa^{-1} = 1 \in I$ forces $I = \langle 1 \rangle$.
- *Proof (of b).* Let $J \leq R$ be a nonzero two-sided ideal, noting that R is noncommutative the claim is that J contains I_n , the $n \times n$ identity matrix, and thus J = R.
 - Pick a nonzero element $M \in I$, then M has a nonzero entry mij.
 - Let A_{ij} be the matrix with a 1 in the i, j position and zeros elsewhere.
 - Left-multiplying $A_{ij}M$ moves row j to row i and zeros out the rest of M.
 - Right-multiplying MA_{ij} moves column *i* to column *j* and zeros out the rest.
 - So $A_{ij}MA_{kl}$ moves entry j, k to i, l and zeros out the rest.
 - So define $B := A_{i,i}MA_{j,i}$, which movies m_{ij} to the i, i position on the diagonal and has zeros elsewhere.
 - Then $m_{ij}^{-1}\varepsilon_{ii} := A_{ii}$ is a matrix with 1 in the *i*, *i* spot for any *i*. Since *I* is an ideal, we have $\varepsilon_{ii} \in I$ for every *i*.
 - We can write the identity I_n as $\sum_{i=1}^n \varepsilon_{ii}$, so $I_n \in I$ and I = R.

7.6.2 Spring 2016 #8

Problem 7.6.1 (?)

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.

A Warning 7.6.1

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

Concepts Used:

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

Solution:

Note: solutions borrowed from folks on Math twitter!

Proof (part 1).

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

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

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

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

Proof (part 2). • First we'll show z = 2(yz): xy + xy = x $\implies xy + xy - x = 0$ $\implies xyz + xyz - xz = 0$ $\implies x(yz + yz - z) = 0$ $\implies yz + yz - z = 0$ since $x \neq 0$ and no zero divisors $\implies 2(yz) = z.$ • Now we'll show z = 2(zy): yz + yz = z $\implies zyz + zyz = zz$ $\implies zyz + zyz - zz = 0$ $\implies (zy + zy - z)z = 0$ $\implies z = 0 \text{ or } zy + zy - z = 0$ no zero divisors . • Then if z = 0, we have yz = 0 = zy and we're done.

• Otherwise, 2(zy) = z, and thus

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

so zy = yz.

Proof (of 2, if R is unital). • If $1 \in R$, 2xy = x $\implies 2xy - x = 0$ $\implies x(2y-1) = 0$ $\implies 2y - 1 = 0$ $x \neq 0$ and no zero divisors $\implies 2y = 1.$ • Now use $1 \cdot z = z \cdot 1$ $\implies (2y)z = z(2y)$ $\implies (y+y)z = z(y+y)$ $\implies yz + yz = zy + zy$ $\implies 2(yz) = 2(zy)$ $\implies 2(yz - zy) = 0$ $\implies yz - zy = 0$, using condition (2).

7.7 Unsorted

7.7.1 Fall 2019 #3

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

- a. Prove that R has characteristic 2.
- b. Prove that R is commutative.

Strategy:

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

Solution:

Proof (of a).

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

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

Proof (of b).

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

7.7.2 Spring 2018 #5

Let

$$M = \left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \quad \text{and} \quad N = \left(\begin{array}{cc} x & u \\ -y & -v \end{array}\right)$$

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

$$MN = \left(\begin{array}{cc} 0 & 0\\ 0 & * \end{array}\right) \implies MN = 0.$$

Solution:

• Multiply everything out to get

$$\begin{bmatrix} ax - by & au - bv \\ cx - dy & cu - dv \end{bmatrix},$$

so it suffices to show cu = dv given

$$ax = by$$
$$cx = dy$$
$$au = bv.$$

• Writing *cu*: - Use that $b \in \mathbb{R}^{\times}$, left-multiply (1) by b^{-1} to get $b^{-1}ax = y$ - Substitute y into (2) to get $cx = d(b^{-1}ax)$. - Since $x \in \mathbb{R}^{\times}$, right-multiply by x^{-1} to get $c = db^{-1}a$ and thus $cu = db^{-1}au$. - Summary: $ax = by \implies b^{-1}ax = y$ $\implies cx = dy = d(b^{-1}ax)$ $\implies c = db^{-1}a$ $\implies cu = db^{-1}au.$ • Writing dv: - Left-multiply (3) by b^{-1} to get $b^{-1}au = v$. - Left-multiply by d to get $db^{-1}au = dv$ – Summary: $au = bv \implies b^{-1}au = v$ $\implies db^{-1}au = dv.$ • So $cu = db^{-1}au = dv.$

7.7.3 Spring 2014 #6

 ${\cal R}$ be a commutative ring with identity and let n be a positive integer.

- a. Prove that every surjective R-linear endomorphism $T: \mathbb{R}^n \to \mathbb{R}^n$ is injective.
- b. Show that an injective R-linear endomorphism of R^n need not be surjective.

3 | Galois Theory

8.1 General Galois Extensions

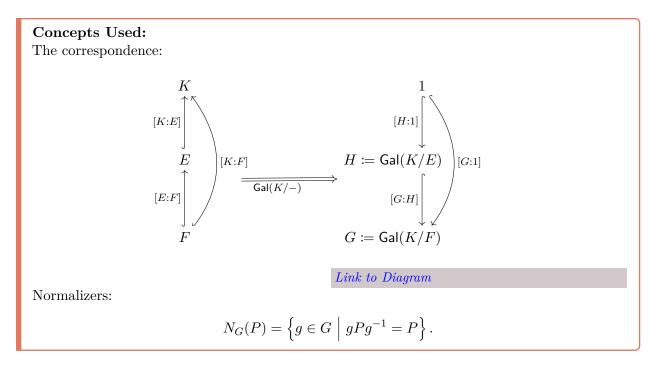
8.1.1 Fall 2021 #4

Recall that for a given positive integer n, the cyclotomic field $\mathbb{Q}(\zeta_n)$ is generated by a primitive n-th root of unity ζ_n .

- a. What is the degree of $Q(\zeta_n)$ over Q?
- b. Define what it means for a finite field extension L/K to be Galois, and prove that the cyclotomic field $Q(\zeta_n)$ is Galois over \mathbb{Q} .
- c. What is the Galois group of $\mathbb{Q}(\zeta_n)$ over \mathbb{Q} ?
- d. How many subfields of $\mathbb{Q}(\zeta_{2021})$ have degree 2 over Q? Note that $2021 = 43 \cdot 47$

8.1.2 Fall 2020 #4

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



Solution:

• Reduce to a group theory problem: [E:F] = [G:H], despite the fact that E/F is not

necessarily Galois. This is because we can count in towers:

$$[K:F] = [K:E][E:F] \implies [G:1] = [K:E][H:1]$$
$$\implies \sharp G = [K:E]\sharp H$$
$$\implies [G:H] = \frac{\sharp G}{\sharp H} = [K:E]$$

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

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

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

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

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

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

8.1.3 Fall 2019 Midterm #9

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

Solution:

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

$$\sigma_{1}(\zeta_{n} + \zeta_{n}^{-1}) = \zeta_{n} + \zeta_{n}^{-1} = \alpha_{1}$$

$$\sigma_{2}(\zeta_{n} + \zeta_{n}^{-1}) = \zeta_{n}^{2} + \zeta_{n}^{-2} = \alpha_{2}$$

$$\sigma_{3}(\zeta_{n} + \zeta_{n}^{-1}) = \zeta_{n}^{3} + \zeta_{n}^{-3} = \alpha_{3}$$

$$\vdots$$

$$\sigma_{n-1}(\zeta_{n} + \zeta_{n}^{-1}) = \zeta_{n}^{n-1} + \zeta_{n}^{-(n-1)} = \zeta_{n}^{-1} + \zeta_{n}^{1} = \alpha_{1}$$

$$\sigma_{n-2}(\zeta_{n} + \zeta_{n}^{-1}) = \zeta_{n}^{n-2} + \zeta_{n}^{-(n-2)} = \zeta_{n}^{-2} + \zeta_{n}^{2} = \alpha_{2}$$

$$\sigma_{n-3}(\zeta_{n} + \zeta_{n}^{-1}) = \zeta_{n}^{n-3} + \zeta_{n}^{-(n-3)} = \zeta_{n}^{-3} + \zeta_{n}^{3} = \alpha_{3}$$

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

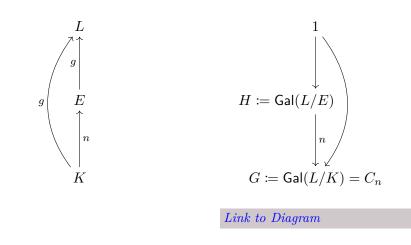
• For *n* not prime, the exact same argument runs through $\varphi(n)$ values of *k* for σ_k , and again yields $\sigma_k(\alpha_1) = \sigma_{\varphi(n)-k}(\alpha_1)$. Matching them up appropriately yields $\varphi(n)/2$ distinct roots.

8.1.4 Fall 2019 Midterm #10

Let L/K be a finite normal extension.

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

Solution: The setup:



Part 1:

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

Part 2:

• Letting $G \coloneqq \mathsf{Gal}(L/K) = C_n$, by elementary group theory we have subgroups $H \coloneqq C_d \leq C_n$ for every d dividing n.

- A observation we'll need: every subgroup is normal here since G is abelian.

- By the fundamental theorem, taking the fixed field of $H \leq \operatorname{Gal}(L/K)$, we obtain some intermediate extension $E := K^H$ fitting into a tower L/E/K.
- By the fundamental theorem, [E:K] = [G:H] = n/d, where we've used that $H \leq G$.
- Letting d range through divisors lets n/d range through divisors, so we get extensions of every degree d dividing n.

8.1.5 Fall 2019 Midterm #8

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

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

8.1.6 Fall 2019 Midterm #7

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

8.1.7 Spring 2012 #4

Let $f(x) = x^7 - 3 \in \mathbf{Q}[x]$ and E/\mathbf{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 $E \neq \mathbf{Q}(\alpha)$.

8.1.8 Fall 2013 #5

Let L/K be a finite extension of fields.

- a. Define what it means for L/K to be *separable*.
- b. Show that if K is a finite field, then L/K is always separable.
- c. Give an example of a finite extension L/K that is not separable.

Solution:

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

- Note: write $g(x) \coloneqq \sum a_k x^k$, so that $f(x) = \sum a_k (x^p)^k = \sum a_k x^{pk}$.

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

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

- Proof of claim: in ch k = p, f inseparable $\implies f(x) = g(x^p)$.
 - Use that f is inseparable iff $gcd(f, f') \neq 1$, and since f is irreducible this forces $f' \equiv 0$, so $ka_k = 0$ for all k.
 - Then $a_k \neq 0$ forces $p \mid k$, so $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots$ and one takes $g(x) \coloneqq \sum a_{kp} x^{kp}$.
- A finite inseparable extension:
 - It's a theorem that finite extensions of perfect fields are separable, so one needs a non-perfect field.

- Take $L/k := \mathbf{F}_p(t^{\frac{1}{p}})/\mathbf{F}_p(t)$, which is a degree p extension (although both fields are infinite are characteristic p).
- Then the minimal polynomial of t is $f(x) := x^p t \in \mathbf{F}_p(t)[x]$, where $f'(x) = px^p \equiv 0$ Alternatively, just note that f factors as $f(x) = (x - t^{\frac{1}{p}})^p$ in L[x], which has multiple roots.

8.1.9 Fall 2012 #4

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

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

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

Solution: Z/2Z?

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

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

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

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

8.2.3 Fall 2020 #3

- a. Define what it means for a finite extension of fields E over F to be a *Galois* extension.
- b. Determine the Galois group of $f(x) = x^3 7$ over **Q**, and justify your answer carefully.
- c. Find all subfields of the splitting field of f(x) over **Q**.

Solution:

Part a:

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

Part b:

- Note f is irreducible by Eisenstein with p = 7, and since **Q** is perfect, irreducible implies separable.
- Writing $L := SF(f)/\mathbf{Q}$, this is a Galois extension:
 - -L is separable: it is a finite extension of a perfect field, which is automatically separable.
 - -L is normal: L is the splitting field of a separable polynomial, and thus normal.
- Since f is degree 3, we have $G := \operatorname{Gal}(L/k) \leq S_3$, and since G is a transitive subgroup the only possibilities are

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

- Factor $x^3 7 = (x \omega)(x \zeta_3 \omega)(x \zeta_3^2 \omega)$ where $\omega := 7^{\frac{1}{3}}$ and ζ_3 is a primitive 3rd root of unity. Then $L = \mathbf{Q}(\zeta_3, \omega)$.
 - Aside: label the roots in this order, so $r_1 = \omega$, $r_2 = \zeta_3 \omega$, $r_3 = \zeta_3^2 \omega$.
- Write $\min_{\omega,\mathbf{Q}}(x) = x^3 7$ and let $L_0/\mathbf{Q} \coloneqq \mathbf{Q}(\omega)/\mathbf{Q}$ yields $[L_0:\mathbf{Q}] = 3$.
- Write $\min_{\zeta_3,\mathbf{Q}}(x) = (x^3 1)/(x 1) = x^2 + x + 1$, and note that this is still the minimal polynomial over L_0 since $L_0 \subseteq \mathbf{R}$ and $\zeta_3 \in \mathbf{C} \setminus \mathbf{R}$. So $[L:L_0] = 2$.
- Counting in towers,

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

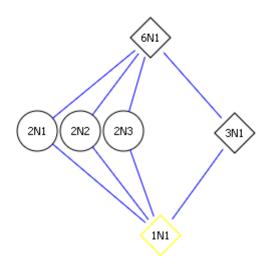
• But $\#S_3 = 6$ and $\#A_3 = 3$, so $G = S_3$.

• Explicitly, since we can write $SF(f) = \mathbf{Q}(\omega, \zeta_3)$, we can find explicit generators:

$$\begin{split} \sigma : &\begin{cases} \omega & \mapsto \omega \\ \zeta_3 & \mapsto \zeta_3 \cdot \zeta_3. \end{cases} & \implies \sigma \sim (1, 2, 3) \\ \tau : &\begin{cases} \omega & \mapsto \omega \\ \zeta_3 & \mapsto \overline{\zeta_3}. \end{cases} & \implies \tau \sim (2, 3). \end{split}$$
 So $G = &\langle \sigma, \tau \mid \sigma^3, \tau^2 \rangle. \end{split}$

Part c:

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



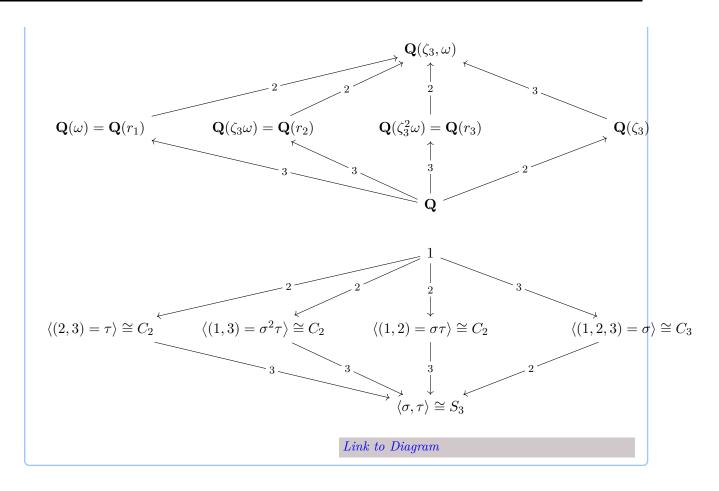
- Note that we can identify
 - $-\tau = (2,3)$ which fixes r_1
 - $-\sigma\tau = (1,2)$ which fixes r_3
 - $-\sigma^2 \tau = (1,3)$ which fixes r_2
 - $-\sigma = (1, 2, 3)$, for which we need to calculate the fixed field. Using that $\sigma(\omega) = \zeta \omega$ and $\sigma(\zeta) = \zeta$, supposing $\sigma(\alpha) = \alpha$ we have

$$\sigma(\alpha) \coloneqq \sigma(a + b\zeta_3 + c\zeta_3^2 + d\omega + e\zeta_3\omega + f\zeta_3^2\omega)$$

= $a + b\zeta_3 + c\zeta_3^2 + d\zeta_3\omega + e\zeta_3^2\omega + f\omega$
 $\implies \alpha = a + b\zeta_3 + c\zeta_3^2 + t_1(\omega + \zeta_3\omega + \zeta_3^2\omega)$
 $\implies \alpha = a + b\zeta_3 + c\zeta_3^2 + t_1\omega(1 + \zeta_3 + \zeta_3^2)$
 $\implies \alpha = a + b\zeta_3 + c\zeta_3^2,$

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

• We thus get the following lattice correspondence:



8.2.4 Spring 2021 #4

Define

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

- a. Find the splitting field K of f over \mathbf{Q} .
- b. Find the Galois group G of f.
- c. Exhibit explicitly the correspondence between subgroups of G and intermediate fields between \mathbf{Q} and K.

Concepts Used:

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

Solution:

• First consider $g(z) := z^2 + 4z + 64$. Applying the quadratic formula yields

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

• Substituting $z = x^2$ yields the splitting field of f as $L \coloneqq \mathbf{Q}(\pm \sqrt{-2 \pm 2i\sqrt{15}})$.

- Note that this factorization shows that f is irreducible over \mathbf{Q} , since the two quadratic factors have irrational coefficients and none of the roots are real.
- Irreducible implies separable over a perfect field, so L/\mathbf{Q} is a separable extension.
- $-\ L$ is the splitting field of a separable polynomial and thus normal, making L Galois.
- In this form, it's not clear what the degree $[L : \mathbf{Q}]$ is, so we can find a better basis by rewriting the roots of g:

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

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

• Counting in towers,

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

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

- So $G := \operatorname{Gal}(L/\mathbf{Q}) \leq S_4$ is a transitive subgroup of size 4, making it either C_4 or C_2^2 .
- Label the roots:

$$r_{1} = \sqrt{5} + i\sqrt{3}$$

$$r_{2} = \sqrt{5} - i\sqrt{3}$$

$$r_{3} = -\sqrt{5} + i\sqrt{3} = -r_{2}$$

$$r_{4} = -\sqrt{5} - i\sqrt{3} = -r_{1}$$

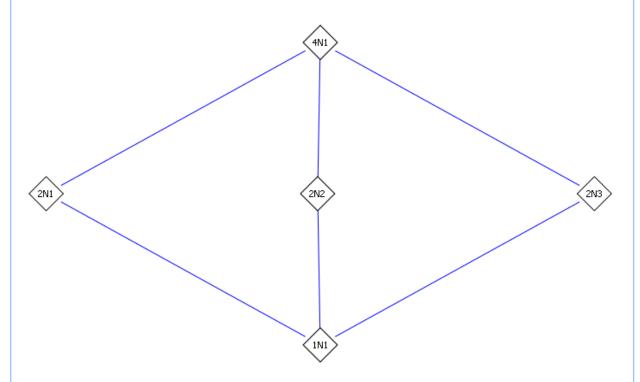
• We can start writing down automorphisms:

$$\begin{aligned} \sigma_1 : \begin{cases} \sqrt{5} & \mapsto -\sqrt{5} \\ i\sqrt{3} & \mapsto i\sqrt{3}. \end{cases} & \sigma_1 \sim (1,3)(2,4) \\ \sigma_2 \begin{cases} \sqrt{5} & \mapsto \sqrt{5} \\ i\sqrt{3} & \mapsto -i\sqrt{3}. \end{cases} & \sigma_2 \sim (1,2)(3,4). \end{aligned}$$

Note that these define automorphisms because we've specified what happens to a basis and they send roots to other roots. • Checking that $\sigma_1^2 = \sigma_2^2 = id$, this produces two distinct order 2 elements, forcing $G \cong C_2^2$ since C_4 only has one order 2 element. Explicitly, we have

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

and the generic subgroup lattice looks like:



- Computing some fixed fields. Write $i\sqrt{3} = x, \sqrt{5} = y$, then elements in the splitting field are of the form $\alpha = 1 + ax + by + cxy$.
 - For σ_1 , we have $x \mapsto -x$, so

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

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

- For σ_2 , we have $y \mapsto -y$, so

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

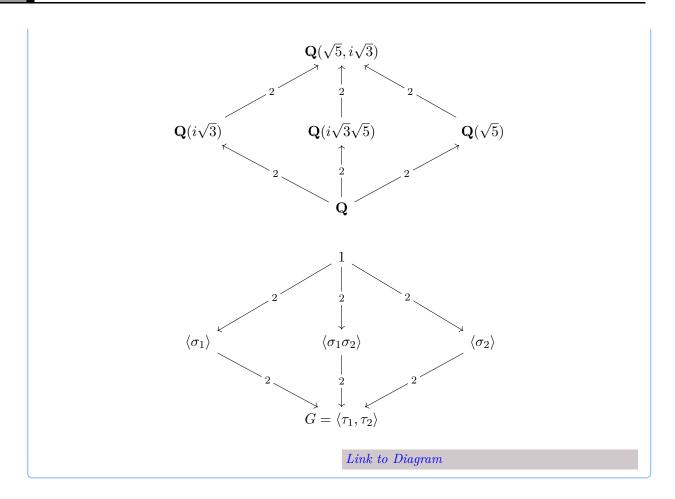
preserving 1 + ax and making the fixed field $\mathbf{Q}(1, x) = \mathbf{Q}(\sqrt{5})$.

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

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

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

• So the lattice correspondence we get here is



8.2.5 Fall 2019 Midterm #6

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

8.2.6 Spring 2018 #2

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

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

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

Solution:

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

$$\alpha_1 = \sqrt{2 + \sqrt{2}}$$
$$\alpha_2 = \sqrt{2 - \sqrt{2}}$$
$$\alpha_3 = -\alpha_1$$
$$\alpha_4 = -\alpha_2.$$

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

Proof (of b).

K is the splitting field of a separable polynomial and thus Galois over \mathbf{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

•
$$\mathbf{Z}/(2) \times \mathbf{Z}/(2)$$

• **Z**/(4)

We can note that g splits over $L \coloneqq \mathbf{Q}(\sqrt{2})$, 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

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

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

Z/(2) × Z/(2)
Z/(4)

We can next check orders of elements. Take

$$\sigma \in \mathsf{Gal}(K/\mathbf{Q})$$
$$\alpha_1 \mapsto \alpha_2.$$

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

$$\sigma^{2}(\alpha_{1}) = \sigma(\alpha_{2})$$

$$= \sigma\left(\frac{\sqrt{2}}{\alpha_{1}}\right)$$

$$= \frac{\sigma(\sqrt{2})}{\sigma(\alpha_{1})}$$

$$= \frac{\sigma(\alpha_{1}^{2} - 2)}{\alpha_{2}}$$

$$= \frac{\alpha_{2}^{2} - 2}{\alpha_{2}}$$

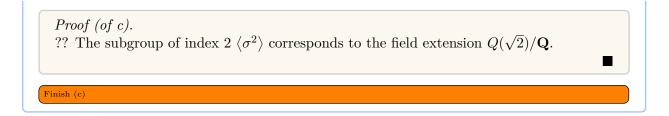
$$= \alpha_{2} - 2\alpha_{2}^{-1}$$

$$= \alpha_{2} - \frac{2\alpha_{1}}{\sqrt{2}}$$

$$= \alpha_{2} - \alpha_{1}\sqrt{2}$$

$$\neq \alpha_{1}.$$

8.2 Gaund Group the Coarder Cofinguististic trictly greater than 2, and thus 4, and thus $\mathsf{Gal}(K/\mathbf{Q}) = 97$ $\left\{ \sigma^k \mid 1 \le k \le 4 \right\} \cong \mathbf{Z}/(4).$



8.2.7 Spring 2020 #4

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

- a. Define what it means for a finite extension field E of a field F to be a Galois extension.
- b. Determine the Galois group $\operatorname{Gal}(E/\mathbf{Q})$ for the polynomial f(x), and justify your answer carefully.
- c. Exhibit a subfield K in (b) such that $\mathbf{Q} \leq K \leq E$ with K not a Galois extension over \mathbf{Q} . Explain.

8.2.8 Spring 2017 #8

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

$$\left(\begin{array}{cc} a & b \\ 0 & 1 \end{array}\right)$$
 where $a \in \mathbf{F}_5^{\times}$ and $b \in \mathbf{F}_5$.

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

8.2.9 Fall 2016 #4

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

- a. Find the splitting field K of f(x) over \mathbf{Q} .
- b. Find the Galois group G of K over \mathbf{Q} .
- c. Exhibit explicitly the correspondence between subgroups of G and intermediate fields between \mathbf{Q} and K.

8.2.10 Spring 2016 #2

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

- a. Find $[K : \mathbf{Q}]$.
- b. Show that K/\mathbf{Q} is Galois, and find the Galois group G of K/\mathbf{Q} .
- c. Exhibit explicitly the correspondence between subgroups of G and intermediate fields between \mathbf{Q} and K.

8.2.11 Fall 2015 #5

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

- a. Find (with justification) the minimal polynomial f(x) of u over \mathbf{Q} .
- b. Show $v \in E$, and show that E is a splitting field of f(x) over **Q**.
- c. Determine the Galois group of E over \mathbf{Q} and determine all of the intermediate fields F such that $\mathbf{Q} \subset F \subset E$.

8.2.12 Spring 2015 #5

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

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

8.2.13 Fall 2014 #3

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

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

8.2.14 Fall 2013 #6

- Let K be the splitting field of $x^4 2$ over **Q** and set $G = \text{Gal}(K/\mathbf{Q})$.
 - a. Show that K/\mathbf{Q} contains both $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt[4]{2})$ and has degree 8 over $\mathbf{Q}/$
 - b. Let $N = \operatorname{Gal}(K/\mathbf{Q}(i))$ and $H = \operatorname{Gal}(K/\mathbf{Q}(\sqrt[4]{2}))$. Show that N is normal in G and NH = G.

Hint: what field is fixed by NH?

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

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

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

8.2.15 Spring 2014 #4

Let $E \subset \mathbf{C}$ denote the splitting field over \mathbf{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 \mathbf{Q} contained in E.

- b. Find the Galois group of $(x^3 11)(x^2 2)$ over **Q**.
- c. Prove that the minimal polynomial of $11^{1/3} + 2^{1/2}$ over **Q** has degree 6.

8.2.16 Spring 2013 #8

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

- a. Show that if r is a root of f in K, then $r^9 = 1$ but $r^3 \neq 1$.
- b. Find $\operatorname{Gal}(K/F)$ and express each intermediate field between F and K as $F(\beta)$ for an appropriate $\beta \in K$.

8.3 Galois Groups: Indirect Computations / Facts

8.3.1 Fall 2019 #7

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

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

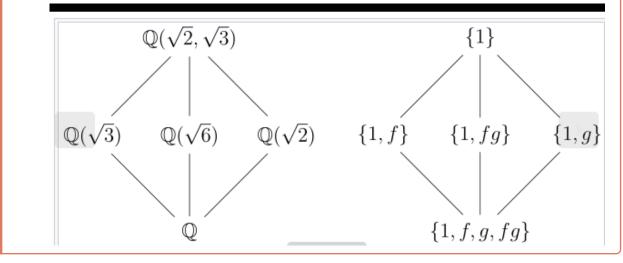
How many subfields are there of $\mathbf{Q}(\zeta_{20})$?

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 \mathbf{F}^{\times} .

•
$$\varphi(p^k) = p^{k-1}(p-1)$$

• The lattice:



Solution:

Let $K = \mathbf{Q}(\zeta)$. Then K is the splitting field of $f(x) = x^n - 1$, which is irreducible over \mathbf{Q} , so K/\mathbf{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, $|\mathsf{Gal}(K/\mathbf{Q})| = [K : \mathbf{Q}] = \varphi(n)$ for the totient function. We can now define maps

$$\tau_j: K \to K$$
$$\zeta \mapsto \zeta^j$$

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 $\min(\zeta, \mathbf{Q})$, and so these are in fact automorphisms of K that fix **Q** and thus elements of $Gal(K/\mathbf{Q})$.

So define a map

$$\theta: \mathbf{Z}_n^{\times} \to K$$
$$[j]_n \mapsto \tau_j.$$

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 $[K : \mathbf{Q}]$ has a basis $\{1, \zeta, \zeta^2, \cdots, \zeta^{n-1}\}$, 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 $1 \le k \le n$. Moreover, since $o(\zeta) = n \in K^{\times}$, we must have $o(\zeta^k) = n \in K^{\times}$ as well. Noting that $\{\zeta^i\}$ 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 $K \cong \mathbf{Z}_{20}^{\times}$ and $\varphi(20) = 8$, so $K \cong \mathbf{Z}_8$, so we have the following subgroups and corresponding intermediate fields:

• $0 \sim \mathbf{Q}(\zeta_{20})$

•
$$\mathbf{Z}_2 \sim \mathbf{Q}(\omega_1)$$

- $\mathbf{Z}_4 \sim \mathbf{Q}(\omega_2)$ $\mathbf{Z}_8 \sim \mathbf{Q}$

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

8.3.2 Fall 2018 #3

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

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

Concepts Used:

• Every quadratic extension over **Q** is Galois.

Solution:

Let L/K/F.

Proof (of a).

False: Take $L/K/F = \mathbf{Q}(\zeta_2, \sqrt[3]{2}) \to \mathbf{Q}(\sqrt[3]{2}) \to \mathbf{Q}$.

Then L/F is Galois, since it is the splitting field of $x^3 - 2$ and **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 $L/K/F = \mathbf{Q}(\sqrt[4]{2}) \rightarrow \mathbf{Q}(\sqrt{2}) \rightarrow \mathbf{Q}$. Then each successive extension is quadratic (thus Galois) but $\mathbf{Q}(\sqrt[4]{2})$ is not the splitting field of any polynomial (noting that it does not split $x^4 - 2$ completely.)

8.3.3 Spring 2018 #3

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

Let $E = E_1 E_2 \subset K$.

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

- a. Show that $H = H_1 \cap H_2$.
- b. Show that H_1H_2 is a subgroup of G.
- c. Show that

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

Concepts Used:

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

Solution:

Proof (of a). By the Galois correspondence, it suffices to show that the fixed field of $H_1 \cap H_2$ is E_1E_2 . Let $\sigma \in H_1 \cap H_2$; then $\sigma \in Aut(K)$ 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 $E_i \supseteq \mathbf{Q}$, so each τ_i fixes \mathbf{Q} and thus σ fixes \mathbf{Q} .

Claim: All elements in this subset commute.

Proof (of claim).

- Let $\sigma = \sigma_1 \sigma_2 \in H_1 H_2$.
- 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 $K/E/\mathbf{Q}$ 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

$$\sigma(x) = x \iff \tau_1 \tau_2(x) = x \iff \tau_2(x) = x$$

$$\&$$

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

8.3.4 Fall 2017 #4

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

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

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

8.3.5 Spring 2017 #7

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

- a. Define what a splitting field of f(x) over F is.
- b. Let F now be a finite field with q elements. Let E/F be a finite extension of degree n > 0. Exhibit an explicit polynomial $g(x) \in F[x]$ such that E/F is a splitting field of g(x) over F. Fully justify your answer.
- c. Show that the extension E/F in (b) is a Galois extension.

8.3.6 Spring 2016 #6

Problem 8.3.1 (?)

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.

Concepts Used:

- If $N \leq G$ is a normal subgroup and $H \leq G$ is any subgroup containing N, then N is normal in H since $hNh^{-1} \subseteq gNg^{-1} = N$.
- In characteristic zero, a polynomial is solvable by radicals iff its Galois group is a solvable group.

Solution:

Let $G \coloneqq \mathsf{Gal}(K/F)$, then it suffices to show that G is always a solvable group, i.e. any group of order n = 2015 is solvable. Factor $2015 = 5 \cdot 13 \cdot 31$ – this is a pqr factorization, and in fact any group with exactly 3 prime factors (so n is squarefree in particular) will be solvable. Let p = 5, q = 13, r = 31 so that p < q < r. We aim to construct a composition series whose successive quotients are simple groups. Applying Sylow 3 yields

- $n_p \mid qr, n_p \equiv 1 \mod p \implies n_5 \mid 13 \cdot 31 = 403 \text{ and } n_5 \equiv 1 \mod 5.$
 - So $n_5 \in \{1, 13, 31\}$ by divisibility and imposing the congruence forces $n_5 \in \{1, 31\}$ since $13 \neq 1 \mod 5$.
- $n_q \mid pr, n_q \equiv 1 \mod q \implies n_{13} \mid 5 \cdot 31 = 155 \text{ and } n_{13} \equiv 1 \mod 13.$
 - So $n_{13} \in \{1, 5, 31\}$ by divisibility and the congruence imposes $n_{13} \in \{1\}$ since $5, 31 \not\equiv 1 \mod 13$. In particular, there is one Sylow 13-subgroup which is normal.

- 8
- $n_r \mid pq, n_r \equiv 1 \mod r \implies n_{31} \mid 5 \cdot 13 = 65 \text{ and } n_{31} \equiv 1 \mod 31.$
 - So $n_{31} \in \{1, 5, 13\}$ by divisibility and the congruence imposes $n_{31} \in \{1\}$ since $5, 13 \not\equiv 1 \mod 31$. In particular, the one Sylow 31-subgroup is normal.

Let H_{13}, H_{31} be the two normal subgroups of G. Taking the quotient $\tilde{G} \coloneqq G/H_{31}$ yields a group of order $5 \cdot 13$, and a similar argument as above using the Sylow theorems shows that \tilde{G} has a normal subgroup of order 13. By the subgroup correspondence theorem, this yields a normal subgroup $N_1 \leq G$ containing H_{31} which has order $13 \cdot 31$. So define $N_2 \coloneqq H_{31}$ to obtain

$$G \supseteq N_1 \supseteq N_2 \coloneqq H_{31} \supseteq 0.$$

Since the quotients N_i/N_{i+1} have prime power order, they are cyclic and thus simple. We know N_1 is normal in G since it came from extending a normal group in a quotient, and we know N_2 is normal in N_1 since it was normal in all of G. So G is solvable.

8.3.7 Fall 2015 #6

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

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 |Gal(K/F)| = 12. Prove that there exists an intermediate field E of K/F with [E:F] = 3.
- c. With K/F as in (b), does an intermediate field L necessarily exist satisfying [L : F] = 2? Give a proof or counterexample.

8.3.8 Fall 2014 #1

Let $f \in \mathbf{Q}[x]$ be an irreducible polynomial and L a finite Galois extension of \mathbf{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 \mathbf{Q} , the conclusion of part (a) need not hold.

8.3.9 Spring 2013 #7

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

- a. Prove that $\operatorname{Gal}(E/B)$ and $\operatorname{Gal}(E/C)$ are normal subgroups of $\operatorname{Gal}(E/\mathbf{Q})$.
- b. Prove that $\operatorname{Gal}(E/B) \cap \operatorname{Gal}(E/C) = \{1\}.$
- c. If $B \cap C = \mathbf{Q}$, show that $\operatorname{Gal}(E/B)\operatorname{Gal}(E/C) = \operatorname{Gal}(E/\mathbf{Q})$.
- d. Under the hypothesis of (c), show that $\operatorname{Gal}(E/\mathbb{Q}) \cong \operatorname{Gal}(E/B) \times \operatorname{Gal}(E/C)$.
- e. Use (d) to describe $\operatorname{Gal}(\mathbf{Q}[\alpha]/\mathbf{Q})$ where $\alpha = \sqrt{2} + \sqrt{3}$.

8.3.10 Fall 2012 #3

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

8.4 *p*th Roots and $x^{p^k} - x$

8.4.1 Spring 2021 #7

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

Strategy:

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

Solution (Likely the 'right' solution):

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

Strategy (for an alternative solution):

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

Concepts Used:

- Reducible: $f \in \mathbf{F}[x]$ is reducible iff there exists $g, h \in \mathbf{F}[x]$ nonconstant with f = gh.
 - Importantly, this factorization needs to happen in $\mathbf{F}[x]$, since we can *always* find such factorizations in the splitting field 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: $f(x) \coloneqq x^p a \in \mathbf{F}[x]$ reducible $\implies f$ has a root in the base field \mathbf{F} .
- Write f(x) = g(x)h(x) and factor $f(x) = \prod_{i=1}^{p} (x r_i) \in SF(f)[x]$ where the r_i are not necessarily distinct roots.
- WLOG, $g(x) = \prod_{i=1}^{\ell} (x r_i)$ for some $1 \le \ell \le p 1$, 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 $R_{\ell} \in \mathbf{F}$ since $g \in \mathbf{F}[x]$.
- 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 *p*th power of R_{ℓ} ?

$$\begin{aligned} R^p_\ell &\coloneqq \left(\prod_{i=1}^{\ell}\right)^l \\ &= \prod_{i=1}^{\ell} r^p_i \\ &= \prod_{i=1}^{\ell} a \\ &= a^{\ell}, \end{aligned}$$

so $R^p_\ell = a^\ell$.

• 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 \mathbf{F} : write

$$a = a^{1}$$

$$= a^{tp+s\ell}$$

$$= a^{tp}a^{s\ell}$$

$$= a^{tp}(a^{\ell})^{s}$$

$$= a^{tp}(R_{\ell}^{p})^{s}$$

$$= (a^{t}R_{\ell}^{s})^{p}$$

$$\coloneqq \beta^{p},$$

so $a = \beta^p$.

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

8.4.2 Fall 2019 #4

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

- a. Prove that n divides $q^k 1$.
- b. Let m be the order of q in $\mathbf{Z}/n\mathbf{Z}^{\times}$. Prove that m divides k.
- c. Prove that m = k.

Revisit, tricky!

Concepts Used:

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

Solution:

Proof (of a).

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

Proof (of b).

• Rephrasing (a), we have

$$n \mid q^{k} - 1 \iff q^{k} - 1 \cong 0 \mod n$$
$$\iff q^{k} \cong 1 \mod n$$
$$\iff m \coloneqq o(q) \mid k.$$

Proof (of c).

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

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

so M is a degree m extension of E.

- Now consider M^{\times} .
- By the argument in (a), n divides $q^m 1 = |M^{\times}|$, 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 $H = \{x \in M \mid x^n 1 = 0\}$, i.e. H contains all solutions to $x^n 1$ in E[x].
- But ζ is one such solution, so $\zeta \in H \subset M^{\times} \subset M$.
- Since $F[\zeta]$ is the smallest field extension containing ζ , we must have F = M, so $\ell = 1$, and k = m.

8.4.3 Spring 2019 #2

Let $F = \mathbf{F}_p$, 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.
- $\mathbf{GF}(p^n)$ is the splitting field of $x^{p^n} x \in \mathbf{F}_p[x]$.
- $x^{p^d} x \mid x^{p^n} x \iff d \mid n$
- $\mathbf{GF}(p^d) \leq \mathbf{GF}(p^n) \iff d \mid n$
- $x^{p^n} x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n.

Solution:

Proof (of a).

We can consider the quotient $K = \frac{\mathbf{F}_p[x]}{\langle \pi(x) \rangle}$, which since $\pi(x)$ is irreducible is an extension of \mathbf{F}_p of degree d and thus a field of size p^d with a natural quotient map of rings $\rho: \mathbf{F}_p[x] \to K$. 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

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

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, \Longrightarrow). Let $L \cong \mathbf{GF}(p^n)$ 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 $\mathbf{F}_p \leq \mathbf{F}_p(\alpha) \leq L$. Then $\mathbf{F}_p \leq \mathbf{F}_p(\alpha) \leq L$, and so $n = [L : \mathbf{F}_p]$ $= [L : \mathbf{F}_p(\alpha)] [\mathbf{F}_p(\alpha) : \mathbf{F}_p]$ $= \ell d$, for some $\ell \in \mathbf{Z}^{\geq 1}$, so d divides n. Proof (of claim, \Leftarrow). $\Leftarrow :$ If $d \mid n$, use the fact (claim) that $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n. So $f = f_i$ for some i.

8.4.4 * Fall 2016 #5

Problem 8.4.1 (?)

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

Solution:

Consider $L := \mathbf{F}_p[x]/(x^{p^{\ell}} - x)$, this yields a field extension L/\mathbf{F}_p with $[L : \mathbf{F}_p] = \ell$ and so $L \cong \mathbf{F}_{p^{\ell}}$ is the splitting field of $x^{p^{\ell}} - x$. Note that $x^{p^{\ell}} - x$ is the product of all monic irreducible polynomials in $\mathbf{F}_p[x]$ of degree dividing ℓ , and since ℓ is prime, the only such polynomials are of degrees 1 or ℓ – this follows because any such polynomial would generate an intermediate extension L' with $L/L'/\mathbf{F}_p$, and multiplicativity in towers yields

$$[L:\mathbf{F}_p] = [L:L'] \cdot [L':\mathbf{F}_p] = \ell,$$

forcing either [L:L'] = 1 or $[L':\mathbf{F}_p] = 1$.

Let P be the desired number of monic irreducible degree ℓ polynomials in $\mathbf{F}_p[x]$. The idea is now to get a formula involving *all* monic irreducible (not necessarily degree ℓ) polynomials and use it to solve for P. By the above observation, we have a factorization

$$x^{p^{\ell}} - x = \prod_{i \in I} f_i(x) = \prod_{i \in I_1} f_i(x) \cdot \prod_{i \in I_2} g_i(x),$$

where I is the set of all monic irreducible polynomials, and the above observation shows $I = I_1 \coprod I_2$ where I_1 are those of degree 1 and I_2 are those of degree ℓ . Taking degrees of both sides yields

$$p^{\ell} = \sum_{i \in I_1} \deg f_i(x) + \sum_{i \in I_2} \deg g_i(x) = \sum_{i \in I_1} 1 + P\ell = \sharp I_1 + P\ell,$$

since each deg $f_i(x) = 1$ and there are $\sharp I_1$ many of them, and deg $g_i(x) = \ell$ and there are P of them. Rearranging yields

$$P\ell = p^{\ell} - \sharp I_1 \implies P = \ell^{-1} \left(p^{\ell} - \sharp I_1 \right),$$

and so it suffices to determine $\sharp I_1$, the number of monic linear irreducible polynomials in $\mathbf{F}_p[x]$. These are all of the form x + a where $a \in \mathbf{F}_p$, and there are p choices for a, so the final count is

$$P = \ell^{-1} \left(p^{\ell} - p \right).$$

8.4.5 * Fall 2013 #7

Let $F = \mathbf{F}_2$ 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.
- \sim

8.5 General Field Extensions

8.5.1 Spring 2020 #3

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

- a. Show that $F(\alpha) = F(\alpha^2)$.
- b. Prove that α^{2020} is algebraic of odd degree over F.

8.5.2 Spring 2012 #1

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

- 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 $\operatorname{Gal}(E/F)$ is nonabelian.

8.5.3 Spring 2019 #8

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

- a. What is the degree of $\mathbf{Q}(\zeta)/\mathbf{Q}$?
- b. How many quadratic subfields of $\mathbf{Q}(\zeta)$ are there?
- c. What is the degree of $\mathbf{Q}(\zeta, \sqrt[4]{2})$ over \mathbf{Q} ?

Concepts Used:

• $\zeta_n := e^{\frac{2\pi i}{n}}$, and ζ_n^k is a primitive *n*th root of unity $\iff \gcd(n,k) = 1$

– In general, ζ_n^k is a primitive $\frac{n}{\gcd(n,k)}$ 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

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

•
$$\operatorname{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong \mathbf{Z}/(n)^{\times}$$

Solution: Let $K = \mathbf{Q}(\zeta)$. Proof (of a).

- $\zeta := e^{2\pi i/8}$ is a primitive 8th root of unity
- The minimal polynomial of an $n{\rm th}$ root of unity is the $n{\rm th}$ 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 $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 4.$

Proof (of b).

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

Proof (of c).

• Let $L = \mathbf{Q}(\zeta, \sqrt[4]{2}).$

Note
$$\mathbf{Q}(\zeta) = \mathbf{Q}(i, \sqrt{2})$$

 $- \mathbf{Q}(i, \sqrt{2}) \subseteq \mathbf{Q}(\zeta)$
 $\diamond \ \zeta_8^2 = i, \text{ and } \zeta_8 = \sqrt{2}^{-1} + i\sqrt{2}^{-1} \text{ so } \zeta_8 + \zeta_8^{-1} = 2/\sqrt{2} = \sqrt{2}.$
 $- \mathbf{Q}(\zeta) \subseteq \mathbf{Q}(i, \sqrt{2}):$
 $\diamond \ \zeta = e^{2\pi i/8} = \sin(\pi/4) + i\cos(\pi/4) = \frac{\sqrt{2}}{2}(1+i).$

• Thus $L = \mathbf{Q}(i, \sqrt{2})(\sqrt[4]{2}) = \mathbf{Q}(i, \sqrt{2}, \sqrt[4]{2}) = \mathbf{Q}(i, \sqrt[4]{2}).$

– Uses the fact that $\mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(\sqrt[4]{2})$ since $\sqrt[4]{2}^2 = \sqrt{2}$

• Conclude

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

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

8.5.4 Fall 2017 #3

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

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

8.5.5 Spring 2015 #2

Let \mathbf{F} be a finite field.

- a. Give (with proof) the decomposition of the additive group $(\mathbf{F}, +)$ 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 $(\mathbf{F}^{\times}, \cdot)$ is cyclic.

8.5.6 Spring 2014 #3

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

- a. Prove that the intermediate field $C_{\text{alg}} \subset C$ consisting of elements algebraic over F is algebraically closed.
- b. Prove that if $F \to E$ is an algebraic extension, there exists a homomorphism $E \to C$ that is the identity on F.

Modules

9.1 Annihilators

9.1.1 Fall 2021 #6

Let R be a commutative ring with unit and let M be an R-module. Define the annihilator of M to be

$$\operatorname{Ann}(M) := \{ r \in R \mid r \cdot m = 0 \text{ for all } m \in M \}$$

- a. Prove that Ann(M) is an ideal in R.
- b. Conversely, prove that every ideal in R is the annihilator of some R-module.
- c. Give an example of a module M over a ring R such that each element $m \in M$ has a nontrivial annihilator $\operatorname{Ann}(m) := \{r \in R \mid r \cdot m = 0\}$, but $\operatorname{Ann}(M) = \{0\}$

9.1.2 Spring 2017 #5

Let R be an integral domain and let M be a nonzero torsion R-module.

- a. Prove that if M is finitely generated then the annihilator in R of M is nonzero.
- b. Give an example of a non-finitely generated torsion R-module whose annihilator is (0), and justify your answer.

9.2 Torsion and the Structure Theorem

9.2.1 * 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

$$\operatorname{Tor}(M) = \{ m \in M \mid \exists r \in R, \ r \neq 0, \ rm = 0 \}.$$

- a. Prove that if R is an integral domain, then Tor(M) is a submodule of M.
- b. Give an example where Tor(M) is not a submodule of M.

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

Concepts Used:

• One-step submodule test.

Solution:

Proof (of a). It suffices to show that

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

We have

$$t_1 \in \operatorname{Tor}(M) \implies \exists s_1 \neq 0 \text{ such that } s_1 t_1 = 0$$

 $t_2 \in \operatorname{Tor}(M) \implies \exists s_2 \neq 0 \text{ such that } s_2 t_2 = 0.$

Since R is an integral domain, $s_1 s_2 \neq 0$. Then

$$s_1 s_2(rt_1 + t_2) = s_1 s_2 rt_1 + s_1 s_2 t_2$$

= $s_2 r(s_1 t_1) + s_1(s_2 t_2)$ since R is commutative
= $s_2 r(0) + s_1(0)$
= 0.

Proof (of b).

Let $R = \mathbf{Z}/6\mathbf{Z}$ as a $\mathbf{Z}/6\mathbf{Z}$ -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.

9.2.2 * Spring 2019 #5

Problem 9.2.1 (?)

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 Tor(M) is 0.
- b. Prove that the rank of M is equal to the rank 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.

Solution:

Proof (of a).

- Suppose toward a contradiction Tor(M) has rank $n \ge 1$.
- Then Tor(M) has a linearly independent generating set $B = {\mathbf{r}_1, \dots, \mathbf{r}_n}$, so in particular

$$\sum_{i=1}^n s_i \mathbf{r}_i = 0 \implies s_i = 0_R \,\forall i.$$

- Let ${\bf r}$ be any of of these generating elements.
- Since $\mathbf{r} \in \text{Tor}(M)$, there exists an $s \in R \setminus 0_R$ such that $s\mathbf{r} = 0_M$.
- Then sr = 0 with s ≠ 0, so {r} ⊆ 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:

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

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

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

- 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

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

which expresses \mathbf{x} as a linear combination of elements in \mathcal{B}' .

Proof (of c).

Notation: Let 0_R denote $0 \in R$ regarded as a ring element, and $\mathbf{0} \in R$ denoted 0_R regarded as a module element (where R is regarded as an R-module over itself)

122

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 $|B| \ge 2$ and let $m_1, m_2 \in B$.
 - Then since R is commutative, $m_2m_1 m_1m_2 = 0$ and this yields a linear dependence
 - So B has only one element m.
 - But then $I = \langle m \rangle = R_m$ is cyclic as an *R* module and thus principal as an ideal of *R*.
 - Now since M was assumed to *not* be principal, M is not free (using the contrapositive of the claim).

Proof (that M is rank 1).

- For any module, we can take an element $\mathbf{m} \in M^{\bullet}$ and consider the cyclic submodule $R\mathbf{m}$.
- Since M is not principle, it is not the zero ideal, and contains at least two elements. So we can consider an element $\mathbf{m} \in M$.
- We have $\operatorname{rank}_R(M) \ge 1$, since $R\mathbf{m} \le M$ 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, $\operatorname{rank}_R(M) \leq 1$.
 - − If we take two elements $\mathbf{m}, \mathbf{n} \in M^{\bullet}$, then since $m, n \in R$ as well, we have nm = mn and so

$$(n)\mathbf{m} + (-m)\mathbf{n} = 0_R = \mathbf{0}$$

is a linear dependence.

M is torsion-free:

- Let $\mathbf{x} \in \text{Tor } M$, 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 $\text{Tor}(M) = \{0_R\}$.

9.2 Torsion and the Structure Theorem

9.2.3 * 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,

$$\operatorname{Hom}_{\mathsf{Set}}(X,\operatorname{Forget}(N)) \xrightarrow{\sim} \operatorname{Hom}_{{}_R\mathsf{Mod}}(M,N).$$

Proof (of b).

• Define the annihilator:

$$\operatorname{Ann}(m) \coloneqq \left\{ r \in R \mid r \cdot m = 0_M \right\} \, \trianglelefteq \, R$$

- Note that $mR \cong R/\operatorname{Ann}(m)$.
- Define the torsion submodule:

$$M_t \coloneqq \left\{ m \in M \mid \operatorname{Ann}(m) \neq 0 \right\} \le M$$

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

Proof (of c).

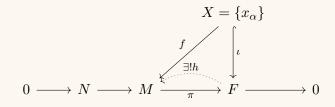
• Let the following be an SES where F is a free R-module:

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

- 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

$$f: X \to M$$
$$x_{\alpha} \mapsto y_{\alpha}.$$

• 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

$$(\pi \circ h)(f) = (\pi \circ h) \left(\sum r_i x_i \right)$$
$$= \sum r_i (\pi \circ h)(x_i),$$

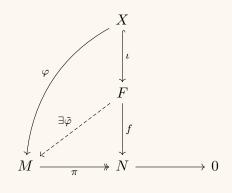
but since $h(x_i) \in \pi^{-1}(x_i)$, we have $(\pi \circ h)(x_i) = x_i$. So this recovers f.

Proof (of c, shorter proof).

- Free implies projective
 - Universal property of **projective** objects: for every epimorphism $\pi: M \to N$ 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 $M \cong M_t \oplus \frac{M}{M_t}$, where M_t is a torsion *R*-module.

Note that by the hint, since R is a PID, it suffices to show that M/M_t is torsionfree.

- Let $m + M_t \in M/M_t$ be arbitrary. Suppose this is a torsion element, the claim is that it must be the trivial coset. This will follow if $m \in M_t$
- Since this is torsion, there exists $r \in R$ such that

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

- 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 $m \in M_t$

9.2.4 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.

9.2.5 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.

9.2.6 Fall 2019 Final #4

Let I = (2, x) be an ideal in $R = \mathbb{Z}[x]$, and show that I is not a direct sum of nontrivial cyclic R-modules.

9.2.7 Fall 2019 Final #5

Let R be a PID.

- a. Classify irreducible *R*-modules up to isomorphism.
- b. Classify indecomposable *R*-modules up to isomorphism.

9.2.8 Fall 2019 Final #6

Let V be a finite-dimensional k-vector space and $T: V \to V$ a non-invertible k-linear map. Show that there exists a k-linear map $S: V \to V$ with $T \circ S = 0$ but $S \circ T \neq 0$.

9.2.9 Fall 2019 Final #7

Let $A \in M_n(\mathbf{C})$ with $A^2 = A$. Show that A is similar to a diagonal matrix, and exhibit an explicit diagonal matrix similar to A.

9.2.10 Fall 2019 Final #10

Show that the eigenvalues of a Hermitian matrix A are real and that $A = PDP^{-1}$ where P is an invertible matrix with orthogonal columns.

9.2.11 Fall 2020 #7

Let $A \in Mat(n \times n, \mathbf{R})$ be arbitrary. Make \mathbf{R}^n into an $\mathbf{R}[x]$ -module by letting $f(x).\mathbf{v} \coloneqq f(A)(\mathbf{v})$ for $f(\mathbf{v}) \in \mathbf{R}[x]$ and $\mathbf{v} \in \mathbf{R}^n$. Suppose that this induces the following direct sum decomposition:

$$\mathbf{R}^{n} \cong \frac{\mathbf{R}[x]}{\langle (x-1)^{3} \rangle} \oplus \frac{\mathbf{R}[x]}{\langle (x^{2}+1)^{2} \rangle} \oplus \frac{\mathbf{R}[x]}{\langle (x-1)(x^{2}-1)(x^{2}+1)^{4} \rangle} \oplus \frac{\mathbf{R}[x]}{\langle (x+2)(x^{2}+1)^{2} \rangle}.$$

- a. Determine the elementary divisors and invariant factors of A.
- b. Determine the minimal polynomial of A.

c. Determine the characteristic polynomial of A.

9.3 Misc/Unsorted

9.3.1 Spring 2017 #3

Problem 9.3.1 (?)

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

- a. Let $I \leq R$ 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.

Solution:

Part a: First, a slightly more advanced argument that gives some intuition as to why this should be true. Let $X = \{g_1, \dots, g_n\} \subseteq M$ be a generating set so that $\operatorname{rank}_R M = n$ and every $m \in M$ can be written as $m = \sum_{i=1}^n r_i m_i$ for some $r_i \in R$. Then $M = Rg_1 \oplus Rg_2 \oplus \cdots Rg_n$, using the notation of Atiyah-MacDonald, where Rm is the cyclic submodule generated by m. In particular, $M \cong R^{\oplus^n}$, and this is true iff M is a free R-module of rank n. So it suffices to show that $M/IM \cong (R/I)^{\oplus^{\ell}}$ for some ℓ and that $\ell = n$. Since free modules are flat, the functor $(-) \otimes_R M$ is left and right exact, so take the short exact sequence

$$0 \to I \hookrightarrow R \twoheadrightarrow R/I \to 0$$

and tensor with M to get

$$0 \to I \otimes_R M \stackrel{\iota}{\hookrightarrow} R \otimes_R M \stackrel{\pi}{\to} (R/I) \otimes_R M \to 0.$$

Noting that $R \otimes_R M \cong M$ by the canonical map $r \otimes m \mapsto rm$ (extended linearly), we have

$$0 \to I \otimes_R M \stackrel{\iota}{\hookrightarrow} M \stackrel{\pi}{\to} (R/I) \otimes_R M \to 0.$$

Now $\iota(i \otimes m) = im$, so the image of ι is precisely IM, and $\operatorname{coker}(\iota) = M/IM$ by definition. By exactness, we must have $\operatorname{coker}(\iota) \cong (R/I) \otimes_R M$, so

$$M/IM \cong (R/I) \otimes_R M.$$

~

But now if $M \cong R^{\oplus^n}$, we can conclude by a direct calculation:

$$M/IM \cong (R/I) \otimes_R M$$

$$\cong (R/I) \otimes_R (R^{\oplus^n})$$

$$\coloneqq (R/I) \otimes_R (R \oplus R \oplus \dots \oplus R)$$

$$\cong ((R/I) \otimes_R R) \oplus ((R/I) \otimes_R R) \oplus \dots \oplus ((R/I) \otimes_R R)$$

$$\cong (R/I) \oplus (R/I) \oplus \dots \oplus (R/I)$$

$$= (R/I)^{\oplus^n},$$

where we've used that $A \otimes (B \oplus C) \cong (A \otimes B) \oplus (A \otimes C)$ and $A \otimes_R R \cong A$ for any *R*-modules A, B, C.

A more direct proof of a: Let $X \coloneqq \{g_1, \cdots, g_n\} \subseteq M$ be a free R-basis for M, so X is R-linearly independent and spans M. The claim is that the cosets X := $\{g_1 + IM, \cdots, g_n + IM\} \subseteq IM$ form a basis for IM.

• Spanning: we want to show

$$m + IM \in M/IM \implies \exists r_k + I \in R/I \text{ such that}$$

 $m + IM = \sum_{k=1}^n (r_K + I)(g_k + IM).$

- Note that the R/I-module structure on M/IM is defined by $(r+I)(m+IM) \coloneqq$ rm + IM.
- Fix m + IM, and use the basis X of M to write $M = \sum_{k=1}^{n} r_k g_k$, since it spans M. - Then

$$m + IM = \left(\sum_{k=1}^{n} r_k g_k\right) + IM = \sum_{k=1}^{n} (r_k g_k + IM) = \sum_{k=1}^{n} (r_k + I)(g_k + IM),$$

so these r_k suffice.

• *Linear independence*: we want to show

$$\sum_{k=1}^{n} (r_k + I)(g_k + IM) = 0_{IM} \implies r_k + I = 0_{R/I} \coloneqq 0 + I \quad \forall k$$

- Expanding the assumption, we have

$$\sum_{k=1}^{n} (r_k + I)(g_k + IM) = 0_{IM} \implies \sum_{k=1}^{n} (r_k g_k) + IM = 0 + IM$$
$$\implies \sum_{k=1}^{n} r_k g_k \in IM,$$

and it suffices to show $r_k \in I$ for all k. - Since $IM \coloneqq \left\{ \sum_{k=1}^N i_k m_k \mid i_k \in I, m_k \in M, N < \infty \right\}$ by definition, we have

$$\sum_{k=1}^n r_k g_k = \sum_{k=1}^N i_k m_k$$

for some $i_k \in I$ and $m_k \in M$ and some finite N.

- Since X is a spanning set for M, we can write expand $m_k = \sum_{k=1}^n r'_k g_k$ for each k and write

$$\sum_{k=1}^{n} r_k g_k = \sum_{k=1}^{N} i_k \left(\sum_{j=1}^{n} r'_j g_j \right) = \sum_{k=1}^{n} \sum_{j=1}^{n} i_k r'_j g_j = \sum_{k=1}^{n} \sum_{j=1}^{n} i_{kj} g_j,$$

where $i_{kj} \coloneqq i_k r'_j \in I$ since I is an ideal.

- By collecting terms for each g_i , we can thus write

$$\sum_{k=1}^n r_k g_k = \sum_{k=1}^n i'_k g_k \implies \sum_{k=1}^n (r_k - i_k) g_k = 0_M,$$

where $i'_k \in I$. Using that the g_k are *R*-linearly independent in *M*, we have $r_k = i_k$ for each *k*, so in fact $r_k \in I$, which is what we wanted to show.

Part b: suppose the result is true for fields. Noting that R/I is a field precisely when I is maximal, suppose R contains a maximal ideal I and let B_1, B_2 be two R-bases for M. By part a, their images B'_1, B'_2 are R/I-bases for M/IM, but since R/I is a field and M/IM is a module over the field k := R/I, the sizes of B'_1 and B'_2 must be the same. This forces the sizes of B_1 and B_2 to be the same.

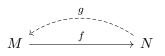
To see that R does in fact contain a maximal ideal, let $S := R^{\times} \setminus R$ be the set of non-units in R. Applying Zorn's lemma shows that S is contained in a proper maximal ideal I, which can be used in the argument above.

9.3.2 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 $N \cong \mathrm{im} f \oplus \ker g$.

Solution:

• We have the following situation:



Link to Diagram

- Claim: im $f + \ker g \subseteq N$, and this is in fact an equality.
 - For $n \in N$, write

$$n = n + (f \circ g)(n) - (f \circ g)(n) = (n - (f \circ g)(n)) + (f \circ g)(n).$$

- The first term is in ker g:

$$g(n - (f \circ g)(n)) = g(n) - (g \circ f \circ g)(n)$$
$$= g(n) - (\mathrm{id}_N \circ g)(n)$$
$$= g(n) - g(n)$$
$$= 0$$

– The second term is clearly in $\operatorname{im} f$.

• Claim: the sum is direct.

- Suppose $n \in \ker(g) \cap \operatorname{im}(f)$, so g(n) = 0 and n = f(m) for some $m \in M$. Then

$$0 = g(n) = g(f(m)) = (g \circ f)(m) = \mathrm{id}_M(m) = m,$$

so m = 0 and since f is a morphism in R-modules, $n \coloneqq f(m) = 0$.

9.3.3 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 **Z**-module. Show that a **Z**-submodule N of M is maximal $\iff \sharp M/N$ is a prime number.
- c. Let M be the **Z**-module of all roots of unity in **C** under multiplication. Show that there is no maximal **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 **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 $G = \{x \in \mathbb{C} \mid x^n = 1 \text{ for some } n \in \mathbb{N}\}$, and suppose H < G is a proper submodule.
- Since $H \neq G$, there is some p and some k such that $\zeta_{p^k} \notin H$.

– Otherwise, if H contains every ζ_{p^k} it contains every ζ_n

Then there must be a prime p such that the $\zeta_{p^k} \notin H$ for all k greater than some constant m – otherwise, we can use the fact that if $\zeta_{p^k} \in H$ then $\zeta_{p^\ell} \in H$ for all $\ell \leq k$, and if $\zeta_{p^k} \in H$ for all p and all k then H = G.

But this means there are infinitely many elements in $G \setminus H$, and so $\infty = [G : H] = |G/H|$ is not a prime. Thus by (b), H can not be maximal, a contradiction.

9.3.4 Fall 2019 Final #2

Consider the **Z**-submodule N of \mathbf{Z}^3 spanned by

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

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

9.3.5 Spring 2018 #6

Let

$$M = \{ (w, x, y, z) \in \mathbf{Z}^4 \mid w + x + y + z \in 2\mathbf{Z} \}$$
$$N = \{ (w, x, y, z) \in \mathbf{Z}^4 \mid 4 \mid (w - x), 4 \mid (x - y), 4 \mid (y - z) \}.$$

a. Show that N is a **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

$\{u_1, u_2, u_3, u_4\}$	is a free basis for M
$\{d_1u_1, d_2u_2, d_3u_3, d_4u_4\}$	is a free basis for ${\cal N}$

c. Use the previous part to describe M/N as a direct sum of cyclic **Z**-modules.

9.3.6 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 $k \ge 0$.

9.3.7 Fall 2016 #6

Problem 9.3.2 (?) Let R be a ring and $f: M \to N$ and $g: N \to M$ be R-module homomorphisms such that $g \circ f = \operatorname{id}_M$. Show that $N \cong \operatorname{im} f \oplus \ker g$.

Solution:

The trick: write down a clever choice of an explicit morphism. Let $P := (f \circ g) : N \to N$, then

$$\Phi: N \to \operatorname{im} f \oplus \ker g$$
$$n \mapsto P(n) + (n - P(n)).$$

The claim is that this is an isomorphism. One first needs to show that this makes sense: P(n) := f(g(n)) is clearly in im f (since f is the last function applied), but it remains to show that $n - P(n) \in \ker g$. This is a direct computation:

$$g(n - P(n)) = g(n) - g(f(g(n))) = g(n) - \mathrm{id}_N(g(n)) = g(n) - g(n) = 0_M,$$

where we've used that g is an R-module morphism in the first step. Also note that Φ is an R-module morphism since it's formed of compositions and sums of such morphisms.

One then has to show that $\inf f \cap \ker g = \{0\}$ – letting n be in this intersection, there exists an $m \in M$ with f(m) = n. Then applying g yields gf(m) = g(n), and the RHS is zero since $n \in \ker g$, and the LHS is $gf(m) = \operatorname{id}_M(m) = m$, so m = 0. Since f is an R-module morphism, we must have f(0) = 0, so n = f(m) = f(0) = 0 as desired. Φ is injective: letting $n \in \ker \Phi$, we have

$$0 = \Phi(n) = P(n) + (n - P(n)) = P(n) - P(n) + n = n.$$

We thus get $N \cong \operatorname{im} \Phi$ and it remains to show Φ is surjective. But this follows for the same reason:

$$n \in N \implies n = n + P(n) - P(n) = P(n) + (n - P(n)) = \Phi(n).$$

9.3.8 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:

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

9.3.9 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 $0 \le i \le n-1$, the module M_{i+1}/M_i is cyclic.

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

9.3.10 Fall 2012 #6

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

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

9.3.11 Fall 2019 Final #1

Let A be an abelian group, and show A is a **Z**-module in a unique way.

9.3.12 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 \mid 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.

10 Linear Algebra: Diagonalizability

10.1 Fall 2017 #7

Problem 10.1.1 (?)

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 $w \in W$. 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 $V_T \cong W_S$ 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.

Concepts Used:

- A representation M of a k-algebra A is a morphism $A \to \operatorname{End}_{k\operatorname{Alg}}(M)$ of k-algebras.
- Simple R-modules M can be written as $M \cong R/I$ for I a maximal ideal.

Solution:

Part a: note that for **F**-modules, i.e. representations of **F**, a morphism $V \to W$ would be an **F**-linear map $\varphi : V \to W$ that commutes with the actions $\mathbf{F} \frown V, W$ that define the module structure, i.e. $\varphi(\lambda \bullet_V v) = \lambda \bullet_W \varphi(v)$ where \bullet_V is the action on V and \bullet_W is the action on W, where $\lambda \in \mathbf{F}, v \in V$.

Here we are considering $\mathbf{F}[x]$ -modules, i.e. representations of the \mathbf{F} -algebra $\mathbf{F}[x]$. Note that $\mathbf{F}[x]$ is generated by 1, x as an \mathbf{F} -algebra, and so specifying a representation M is equivalent to specifying an action by scalars $\mathbf{F} \curvearrowright M$ and an action $x \curvearrowright M$.

Note that a morphism $R: V_T \to W_S$ of $\mathbf{F}[x]$ -modules must in particular be a morphism of the underlying **F**-modules V and W, since **F** can be identified with the constant polynomials in $\mathbf{F}[x]$. Thus it is necessary for R to be **F**-linear.

To see that we must have RS = ST, note that given an action of x on W and V, we must have $R(x \bullet_V v) = x \bullet_W R(v)$. Since $x \bullet_V v \coloneqq T(v)$ and $x \bullet_W w \coloneqq S(w)$, we must have

$$R(T(v)) = R(x \bullet_V v) = x \bullet_W R(v) = S(R(V)) \implies RT = SR.$$

This shows necessity, sufficiency follows because if RT = SR then a similar argument in reverse

shows R(xv) = xR(v) must hold.

Part b:

 \implies : note that $V_T \cong W_S$ forces $\dim_{\mathbf{F}} V = \dim_{\mathbf{F}} W$, so T, S must be square matrices. By part a, such an isomorphism is a isomorphism $P: V \to W$ of \mathbf{F} -modules with PT = SP, which has an inverse $P^{-1}: W \to V$. Choosing \mathbf{F} -bases for V and W, P is an invertible square matrix, so

$$PT = SP \implies P^{-1}PT = P^{-1}SP \implies T = P^{-1}SP.$$

 \Leftarrow : given such a morphism $P: V \to W$ of **F**-modules with $T = P^{-1}SP$, running the above argument backwards we have

$$T = P^{-1}SP \implies PT = PP^{-1}SP \implies PT = SP,$$

and by part a P defines a morphism of $\mathbf{F}[x]$ -modules. A similar argument with P^{-1} produces an inverse morphism, so P yields an *isomorphism* of $\mathbf{F}[x]$ -modules.

> A shorter argument: $V_T \cong W_S \implies$ they have the same invariant factor decompositions $\implies T, S$ have the same rational canonical form \implies they are similar matrices by linear algebra. Conversely, if T, S are similar then $\exists P$ with $T = P^{-1}SP \implies$ PT = SP by definition of similarity.

Part c: let $\mathbf{F} = \mathbf{R}$; by the classification of modules over a PID, any $\mathbf{R}[t]$ -module M has an invariant factor factor decomposition

$$M \cong \mathbf{R}[t]^n \oplus \frac{\mathbf{R}[t]}{\langle f_1 \rangle} \oplus \cdots \oplus \frac{\mathbf{R}[t]}{\langle f_\ell \rangle}, \qquad f_1 \mid f_2 \mid \cdots \mid f_\ell$$

as $\mathbf{R}[t]$ -modules. Simple modules M correspond to $\mathbf{R}[t]/I$ for I a single maximal ideal, and since $\mathbf{R}[t]$ is a PID maximals are prime and thus $I = \langle f \rangle$ for some irreducible polynomial. So let $f(x) = x^2 + 1$, it then suffices to find a matrix $A \in \text{End}(V)$ which has f as its characteristic polynomial – this follows since the characteristic polynomial is $\prod_{i=1}^{\ell} f_i$ in the decomposition above, so we're forcing $\ell = 1$ and $f_1 = f_{\ell} = f$ with n = 0 to get $M \cong \mathbf{R}[t]/\langle f \rangle$. So take

$$T \coloneqq \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

Part d: suppose dim_{**F**} V = 2 and V_T is simple, $V_T \cong \mathbf{F}[x]/I$ for I a maximal ideal. By the invariant factor decomposition, the characteristic polynomial equals the minimal polynomial since I must be generated by an irreducible polynomial. So T is diagonalizable (e.g. by examining the JCF), and in particular $V_T \cong E_1 \oplus E_2$ is a sum of its eigenspaces since **F** is algebraically closed. However, this contradicts simplicity, since T-invariant subspaces of V correspond to $\mathbf{C}[x]$ -submodules of V_T , and E_1 is a 1-dimensional such space.

10.2 Spring 2015 #3

Let F be a field and V a finite dimensional F-vector space, and let $A, B : V \to V$ be commuting F-linear maps. Suppose there is a basis \mathcal{B}_1 with respect to which A is diagonalizable and a basis \mathcal{B}_2 with respect to which B is diagonalizable.

Prove that there is a basis \mathcal{B}_3 with respect to which A and B are both diagonalizable.

10.3 Fall 2016 #2

Let A, B be two $n \times n$ matrices with the property that AB = BA. Suppose that A and B are diagonalizable. Prove that A and B are *simultaneously* diagonalizable.

10.4 Spring 2019 #1

Let A be a square matrix over the complex numbers. Suppose that A is nonsingular and that A^{2019} is diagonalizable over **C**.

Show that A is also diagonalizable over \mathbf{C} .

Concepts Used:

- A is diagonalizable iff $\min_A(x)$ is separable.
 - See further discussion here.

Solution:

Claim: If $A \in GL(m, \mathbf{F})$ is invertible and A^n/\mathbf{F} is diagonalizable, then A/\mathbf{F} is diagonalizable.

Proof (of claim). • Let $A \in GL(m, \mathbf{F})$.

• Since A^n is diagonalizable, $\min_{A^n}(x) \in \mathbf{F}[x]$ 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 $\{\lambda_i\}_{i=1}^m \subset \mathbf{F}$ are the **distinct** eigenvalues of A^n .

- Moreover $A \in \operatorname{GL}(m, \mathbf{F}) \implies A^n \in \operatorname{GL}(m, \mathbf{F})$: A is invertible $\iff \det(A) = d \in \mathbf{F}^{\times}$, and so $\det(A^n) = \det(A)^n = d^n \in \mathbf{F}^{\times}$ using the fact that the determinant is a ring morphism det : $\operatorname{Mat}(m \times m) \to \mathbf{F}$ and \mathbf{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 $k \ge 0$. Thus the *m* terms in the product correspond to precisely *m* distinct linear factors.
- We can now construct a polynomial that annihilates A, namely

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

where we can note that $q_A(A) = \min_{A^n}(A^n) = 0$, and so $\min_A(x) | q_A(x)$ by minimality.

Claim: $q_A(x)$ has exactly nm distinct linear factors in $\overline{\mathbf{F}}[x]$

- 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

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

where we now use the fact that $i \neq j \implies \lambda_i^{\frac{1}{n}} \neq \lambda_j^{\frac{1}{n}}$. Thus no term in the above product appears as a factor in $x^n - \lambda_j$ for $j \neq i$.

• For the second claim, we can check that $\frac{\partial}{\partial x} (x^n - \lambda_i) = nx^{n-1} \neq 0 \in \mathbf{F}$, and $gcd(x^n - \lambda_i, nx^{n-1}) = 1$ since the latter term has only the roots x = 0 with multiplicity n - 1, whereas $\lambda_i \neq 0 \implies$ zero is not a root of $x^n - \lambda_i$.

But now since $q_A(x)$ has exactly distinct linear factors in $\overline{\mathbf{F}}[x]$ and $\min_A(x) \mid q_A(x)$, $\min_A(x) \in \mathbf{F}[x]$ can only have distinct linear factors, and A is thus diagonalizable over \mathbf{F} .

11 Linear Algebra: Misc

11.1 * Spring 2012 #6

Let k be a field and let the group $G = GL(m,k) \times GL(n,k)$ acts on the set of $m \times n$ matrices $M_{m,n}(k)$ as follows:

$$(A,B) \cdot X = AXB^{-1}$$

where $(A, B) \in G$ and $X \in M_{m,n}(k)$.

- a. State what it means for a group to act on a set. Prove that the above definition yields a group action.
- b. Exhibit with justification a subset S of $M_{m,n}(k)$ which contains precisely one element of each orbit under this action.

11.2 * Spring 2014 #7

Let $G = GL(3, \mathbf{Q}[x])$ be the group of invertible 3×3 matrices over $\mathbf{Q}[x]$. For each $f \in \mathbf{Q}[x]$, let S_f be the set of 3×3 matrices A over $\mathbf{Q}[x]$ such that det(A) = cf(x) for some nonzero constant $c \in \mathbf{Q}$.

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.
 - 11.3 Fall 2012 #7

Let k be a field of characteristic zero and $A, B \in M_n(k)$ be two square $n \times n$ matrices over k such that AB - BA = A. Prove that det A = 0.

Moreover, when the characteristic of k is 2, find a counterexample to this statement.

~

11.4 Fall 2012 #8

Prove that any nondegenerate matrix $X \in M_n(\mathbf{R})$ can be written as X = UT where U is orthogonal and T is upper triangular.

11.5 Fall 2012 #5

Let U be an infinite-dimensional vector space over a field k, $f : U \to U$ a linear map, and $\{u_1, \dots, u_m\} \subset U$ vectors such that U is generated by $\{u_1, \dots, u_m, f^d(u_1), \dots, f^d(u_m)\}$ 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 $v_1, \dots, v_n, f^d(v_1), \dots, f^d(v_n)$ for some $d \in \mathbb{N}$, and
- 2. W is finite-dimensional.

Moreover, prove that for any other decomposition $U \cong V' \oplus W'$, one has $W' \cong W$.

11.6 Fall 2015 #7

- a. Show that two 3×3 matrices over **C** are similar \iff their characteristic polynomials are equal and their minimal polynomials are equal.
- b. Does the conclusion in (a) hold for 4×4 matrices? Justify your answer with a proof or counterexample.

11.7 Fall 2014 #4

Let F be a field and T an $n \times n$ matrix with entries in F. Let I be the ideal consisting of all polynomials $f \in F[x]$ such that f(T) = 0.

Show that the following statements are equivalent about a polynomial $g \in I$:

- a. g is irreducible.
- b. If $k \in F[x]$ is nonzero and of degree strictly less than g, then k[T] is an invertible matrix.

~

 \sim

11.8 Fall 2015 #8

Let V be a vector space over a field F and V^{\vee} its dual. A symmetric bilinear form (-, -) on V is a map $V \times V \to F$ satisfying

$$(av_1 + bv_2, w) = a(v_1, w) + b(v_2, w)$$
 and $(v_1, v_2) = (v_2, v_1)$

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

$$W^{\perp} \coloneqq \left\{ v \in V \mid (v, w) = 0 \text{ for all } w \in W \right\}.$$

- a. Show that if X, Y are subspaces of V with $Y \subset X$, then $X^{\perp} \subseteq Y^{\perp}$.
- b. Define an injective linear map

$$\psi: Y^{\perp}/X^{\perp} \hookrightarrow (X/Y)^{\vee}$$

which is an isomorphism if V is finite dimensional.

11.9 Fall 2018 #4

Let V be a finite dimensional vector space over a field (the field is not necessarily algebraically closed).

Let $\varphi : V \to V$ be a linear transformation. Prove that there exists a decomposition of V as $V = U \oplus W$, where U and W are φ -invariant subspaces of V, $\varphi|_U$ is nilpotent, and $\varphi|_W$ is nonsingular.

Revisit.

Solution:

Let m(x) be the minimal polynomial of φ . If the polynomial f(x) = x doesn't divide m, then f does not have zero as an eigenvalue, so φ is nonsingular and since 0 is nilpotent, $\varphi + 0$ works. Otherwise, write $\varphi(x) = x^m \rho(x)$ where $gcd(x, \rho(x)) = 1$. Then

Then

$$V \cong \frac{k[x]}{m(x)} \cong \frac{k[x]}{(x^m)} \oplus \frac{k[x]}{(\rho)} \coloneqq U \oplus W$$

by the Chinese Remainder theorem.

We can now note that $\varphi|_U$ is nilpotent because it has characteristic polynomial x^m , and $\varphi|_W$ is nonsingular since $\lambda = 0$ is not an eigenvalue by construction.

11.10 Fall 2018 #5

Let A be an $n \times n$ matrix.

- a. Suppose that v is a column vector such that the set $\{v, Av, ..., A^{n-1}v\}$ is linearly independent. Show that any matrix B that commutes with A is a polynomial in A.
- b. Show that there exists a column vector v such that the set $\{v, Av, ..., A^{n-1}v\}$ is linearly independent \iff the characteristic polynomial of A equals the minimal polynomial of A.

Concepts Used:

- Powers of A commute with polynomials in A.
- The image of a linear map is determined by the image of a basis

Strategy:

- Use Cayley-Hamilton to relate the minimal polynomial to a linear dependence.
- Get a lower bound on the degree of the minimal polynomial.
- Use $A \curvearrowright k[x]$ to decompose into cyclic k[x]-modules, and use special form of denominators in the invariant factors.
- Reduce to monomials.

Solution:

Proof (of a). Letting **v** be fixed, since $\{A^j \mathbf{v}\}$ 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

$$BA^{k}\mathbf{v} = A^{k}B\mathbf{v}$$
$$= A^{k}p(A)\mathbf{v}$$
$$= p(A)A^{k}\mathbf{v}$$

so B = p(A) as operators since their actions agree on every basis vector in V.

Proof (of b, \Longrightarrow).

- If $\{A^j \mathbf{v}_k \mid 0 \le j \le n-1\}$ 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.

 $Proof \ (of \ b, \ \Leftarrow=).$

- 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 $V = k[x] \frown \mathbf{v}$ 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

$$V \cong k[x] \frown \mathbf{v}$$
$$\coloneqq \left\{ f(x) \frown \mathbf{v} \mid f \in k[x] \right\}$$
$$= \sup_{k} \left\{ x^{k} \frown \mathbf{v} \mid k \ge 0 \right\}$$
$$\coloneqq \sup_{k} \left\{ A^{k} \mathbf{v} \mid k \ge 0 \right\},$$

where we've used that x acts by A and thus x^k acts by A^k .

• Moreover, we can note that if $\ell \ge \deg \chi_A(x)$, then A^{ℓ} is a linear combination of $\{A^j \mid 0 \le j \le n-1\}$, and so

$$V \cong \sup_{k} \left\{ A^{\ell} \mathbf{v} \mid \ell \ge 0 \right\}$$
$$= \sup_{k} \left\{ A^{\ell} \mathbf{v} \mid 1 \le \ell \le n - 1 \right\}$$

11.11 Fall 2019 #8

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

$$\Lambda \coloneqq \left\{ \sum r_i e_i \mid r_i \in \mathbf{Z} \right\}$$

Let \cdot be a non-degenerate $(v \cdot w = 0 \text{ for all } w \in V \iff v = 0)$ 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

$$\Lambda^{\vee} \coloneqq \{ v \in V \mid v \cdot x \in \mathbf{Z} \text{ for all } x \in \Lambda \}.$$

- a. Show that $\Lambda \subset \Lambda^{\vee}$.
- b. Prove that $\det M \neq 0$ and that the rows of M^{-1} span Λ^{\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 $r_i \in \mathbf{Z}$ for all i.
- Then if $\mathbf{x} = \sum_{j=1}^{n} s_j \mathbf{e}_j \in \Lambda$ is arbitrary, we have $s_j \in \mathbf{Z}$ for all j and

$$\langle \mathbf{v}, \mathbf{x} \rangle = \left\langle \sum_{i=1}^{n} r_i \mathbf{e}_i, \sum_{j=1}^{n} s_j \mathbf{e}_j \right\rangle$$
$$= \sum_{i=1}^{n} \sum_{j=1}^{n} r_i s_j \langle \mathbf{e}_i, \mathbf{e}_j \rangle \in \mathbf{Z}$$

since this is a sum of products of integers (since $\langle \mathbf{e}_i, \mathbf{e}_j \rangle \in \mathbf{Z}$ 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

$$M\mathbf{v} = 0 \implies \begin{bmatrix} \mathbf{e}_1 \cdot \mathbf{e}_1 & \mathbf{e}_1 \cdot \mathbf{e}_2 & \cdots \\ \mathbf{e}_2 \cdot \mathbf{e}_1 & \mathbf{e}_2 \cdot \mathbf{e}_2 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \end{bmatrix} = \mathbf{0}$$
$$\implies \sum_{j=1}^n v_j \langle \mathbf{e}_k, \ \mathbf{e}_j \rangle = 0 \quad \text{for each fixed} \quad k.$$

• 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

$$M\mathbf{x} = 0 \implies A^t A \mathbf{x} = 0$$
$$\implies \mathbf{x}^t A^t A \mathbf{x} = 0$$
$$\implies \|A\mathbf{x}\|^2 = 0$$
$$\implies A \mathbf{x} = 0$$
$$\implies \mathbf{x} = 0,$$

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 *i*th column.

Claim: The rows of A^{-1} span Λ^{\vee} . Equivalently, the columns of A^{-t} span Λ^{\vee} .

• Let $B = A^{-t}$ and let \mathbf{b}_i denote the columns of B, so im $B = \text{span} \{\mathbf{b}_i\}$.

• Since $A \in GL(n, \mathbb{Z})$, $A^{-1}, A^t, A^{-t} \in GL(n, \mathbb{Z})$ as well.

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

and

~

$$B^{t}A = (A^{-t})^{t}A = A^{-1}A = I$$
$$\implies \mathbf{b}_{i} \cdot \mathbf{e}_{j} = \delta_{ij} \in \mathbf{Z}$$
$$\implies \operatorname{im} B \subseteq \operatorname{span} \Lambda^{\vee}.$$

11.12 Spring 2013 #6

Let V be a finite dimensional vector space over a field F and let $T: V \to V$ be a linear operator with characteristic polynomial $f(x) \in F[x]$.

- a. Show that f(x) is irreducible in $F[x] \iff$ there are no proper nonzero subspaces W < V with $T(W) \subseteq W$.
- b. If f(x) is irreducible in F[x] and the characteristic of F is 0, show that T is diagonalizable when we extend the field to its algebraic closure.

Is there a proof without matrices? What if V is infinite dimensional?

How to extend basis?

Concepts Used:

- Every $\mathbf{v} \in V$ is *T*-cyclic $\iff \chi_T(x)/\mathbf{k}$ is irreducible.
 - \implies : Same as argument below.
 - \iff : 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 square-free in $\overline{F}[x]$?

Solution:

Let f be the characteristic polynomial of T.

 \sim

- 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 $g \coloneqq \chi_{V,T}(x) \Big|_W \colon W \to W$ is a linear operator on W.

Claim: g divides f in $\mathbf{F}[x]$ 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, $j \ge 1$.
- 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 $j \ge 1$ in the extended basis.)

• 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 $\deg(\det(D xI)) \ge 1$ and so $\chi_{T,W}(x)$ is a proper divisor of $\chi_{T,V}(x)$.
- Thus f is reducible.

Why?

Proof (of a, \Leftarrow). • Suppose f is reducible, then we will produce a proper T-invariant subspace. • Claim: if f is reducible, there exists a nonzero, noncyclic vector **v**. • Then $\operatorname{span}_k \{T^j \mathbf{v}\}_{j=1}^d$ is a T-invariant subspace that is nonzero, and not the entire space since \mathbf{v} is not cyclic. Proof (of b). • Let $\min_{T,F}(x)$ be the minimal polynomial of T and $\chi_{T,F}(x)$ be its characteristic polynomial. • By Cayley-Hamilton, $\min_{T,F}(x)$ divides $\chi_{T,F}$ • Since $\chi_{T,F}$ is irreducible, these polynomials are equal. • Claim: T/F is diagonalizable $\iff \min_{T,F}$ splits over F and is squarefree. • Replace F with its algebraic closure, then $\min_{T,F}$ splits. • Claim: in characteristic zero, every irreducible polynomial is separable - Proof: it must be the case that either gcd(f, f') = 1 or $f' \equiv 0$, where the second case only happens in characteristic p > 0. - The first case is true because deg $f' < \deg f$, and if gcd(f, f') = p, then $\deg p < \deg f$ and $p \mid f$ forces p = 1 since f is irreducible. • So $\min_{T,F}$ splits into distinct linear factors • Thus T is diagonalizable.

11.13 Fall 2020 #8

Let $A \in Mat(n \times n, \mathbb{C})$ such that the group generated by A under multiplication is finite. Show that

$$\operatorname{Tr}(A^{-1}) = \overline{\operatorname{Tr}(A)},$$

where $\overline{(-)}$ denotes taking the complex conjugate and $\operatorname{Tr}(-)$ is the trace.

12 Linear Algebra: Canonical Forms

12.1 Fall 2021 #3

What is the Jordan normal form over \mathbb{C} of a 7×7 matrix A which satisfies all of the following conditions:

- a. A has real coefficients,
- b. rkA = 5,
- c. $rkA^2 = 4$,
- d. rkA I = 6,
- e. rk $A^3 I = 4$,
- f. tr A = 1?

Solution:

- We'll use rank-nullity throughout: rank $M + \dim \ker M = 7$.
- Also note that

$$Av = \lambda v \implies A^n v = A^{n-1}Av = A^{n-1}\lambda v = \dots = \lambda^n v,$$

so if $\lambda \in \operatorname{Spec}(A)$ then $\lambda^n \in \operatorname{Spec}(A^n)$. Conversely, $\lambda \in \operatorname{Spec}(A^n) \implies \lambda^{\frac{1}{n}} \in \operatorname{Spec}(A)$, which we'll use several times.

- Since $5 = \operatorname{rank} A = \operatorname{rank} (A 0 \cdot I)$, we have dim ker $(A 0 \cdot I) = 2$ contributing an eigenvalue of $\lambda = 0$ with multiplicity 2.
- Since $4 = \operatorname{rank} A^2 = \operatorname{rank} (A^2 0 \cdot \lambda) = \operatorname{rank} (A 0 \cdot \lambda)^2$, we have that dim ker $(A 0 \cdot I)^2 = 3$. Since dim ker $(A - 0 \cdot I)^1 = 2 < 3$, this means there is 1 generalized eigenvector associated to $\lambda = 0$.
- Since $6 = \operatorname{rank}(A 1 \cdot I)$, dim ker $(A 1 \cdot I) = 1$, contributing $\lambda = 1$ with multiplicity 1.
- Since rank $(A^3 1 \cdot I) = 4$, we have dim ker $(A^3 1 \cdot I) = 3$, contributing $\lambda = 1$ now to Spec (A^3) instead of Spec(A). Thus some unknown cube roots of 1 are contributed to Spec(A), so any of $1 = \zeta_3^0, \zeta_3, \zeta_3^2$ are possibilities at this point. Call these three contributions z_1, z_2, z_3 , which may not be distinct.
- Now use that $tr(A) = \sum_{i=1}^{n} \lambda_i$ is the sum of the diagonal on JCF(A), using that trace is a similarity invariant, to write

$$1 = tr(A) = (0+0) + (0) + (1) + (z_1 + z_2 + z_3) \implies z_1 + z_2 + z_3 = 0$$

which is actually enough to force $z_1 = 1, z_2 = \zeta_3, z_3 = \zeta_3^2$, since no other combination sums to zero. That $1 + \zeta_3 + \zeta_3^2 = 0$ is a general fact.

- Since $\lambda = 1$ occurs twice as an eigenvalue but dim ker $(A 1 \cdot I) = 1$, the two copies of $\lambda = 1$ must occur in a nontrivial Jordan block.
- So we get a Jordan form

12.2 *	Spring	2012	#8
--------	--------	------	----

Let V be a finite-dimensional vector space over a field k and $T: V \to V$ a linear transformation.

- a. Provide a definition for the minimal polynomial in k[x] for T.
- b. Define the *characteristic polynomial* for T.
- c. Prove the Cayley-Hamilton theorem: the linear transformation T satisfies its characteristic polynomial.

12.3 * Spring 2020 #8

Let $T: V \to V$ be a linear transformation where V is a finite-dimensional vector space over **C**. Prove the Cayley-Hamilton theorem: if p(x) is the characteristic polynomial of T, then p(T) = 0. You may use canonical forms.

12.4 * Spring 2012 #7

Consider the following matrix as a linear transformation from $V\coloneqq {f C}^5$ 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 $\mathbf{C}[x]$ -modules.
- c. Find the Jordan canonical form of A.

12.5 Fall 2019 Final #8

Exhibit the rational canonical form for

- A ∈ M₆(Q) with minimal polynomial (x − 1)(x² + 1)².
 A ∈ M₁₀(Q) with minimal polynomial (x² + 1)²(x³ + 1).

12.6 Fall 2019 Final #9

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

	$\begin{pmatrix} 2 \end{pmatrix}$	0	0	0	
A =	1	1	0	0	
$A \equiv$	$\begin{vmatrix} 1\\ -2 \end{vmatrix}$	-2	0	1	.
	$\begin{pmatrix} -2 \end{pmatrix}$	0	-1	-2)

12.7 Spring 2016 #7

Let $D = \mathbf{Q}[x]$ and let M be a $\mathbf{Q}[x]$ -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.

12.8 Spring 2020 #7

Let

$$A = \begin{bmatrix} 2 & 0 & 0 \\ 4 & 6 & 1 \\ -16 & -16 & -2 \end{bmatrix} \in M_3(\mathbf{C}).$$

- a. Find the Jordan canonical form J of A.
- b. Find an invertible matrix P such that $P^{-1}AP = J$.
- c. Write down the minimal polynomial of A.

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

12.9 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 $F = \mathbf{Q}$,
- b. When $F = \mathbf{F}_p$.

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

$$B\mathbf{x} = \lambda \mathbf{x}$$

$$\iff (A+I)\mathbf{x} = \lambda \mathbf{x}$$

$$\iff A\mathbf{x} = (\lambda - 1)\mathbf{x}$$

so we will find the eigenvalues of B and subtract one from each.

- Note that $B\mathbf{v} = [\sum v_i, \sum v_i, \cdots, \sum v_i]$, 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 $\mathbf{p}_i \coloneqq \mathbf{e}_1 - \mathbf{e}_{i+1} = [1, 0, 0, \dots, 0 - 1, 0, \dots, 0]$ 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,

$$Spec(B) \coloneqq \{(\lambda_i, m_i)\} = \{(p, 1), (0, p - 1)\} \implies \chi_B(x) = (x - p)x^{p-1}$$
$$\implies Spec(A) = \{(p - 1, 1), (-1, p - 1)\} \implies \chi_A(x) = (x - p + 1)(x + 1)^{p-1}$$

• The dimensions of eigenspaces are preserved, thus

$$JCF_{\mathbf{Q}}(A) = J_{p-1}^{1} \oplus (p-1)J_{-1}^{1} = \begin{bmatrix} p-1 & 0 & 0 & \cdots & 0 & 0\\ \hline 0 & -1 & 0 & 0 & 0 & 0\\ \hline 0 & 0 & -1 & 0 & 0 & 0\\ \hline 0 & 0 & 0 & \cdots & \ddots & \ddots & 0\\ \hline 0 & 0 & 0 & 0 & \cdots & -1 & 0\\ \hline 0 & 0 & 0 & 0 & \cdots & 0 & -1 \end{bmatrix}$$

• The matrix P such that $A = PJP^{-1}$ will have columns the bases of the generalized eigenspaces.

- 12
- 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

$$B\mathbf{p}_i = [1 + 0 + \dots + 0 + (-1) + 0 + \dots + 0] = [0, 0, \dots, 0]$$

- 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

det	$ \begin{array}{c} -1 \\ 0 \\ 0 \end{array} $	$ \begin{array}{c} 1 \\ 0 \\ -1 \\ 0 \\ \vdots \\ 0 \end{array} $	$ \begin{array}{c} 0 \\ 0 \\ -1 \end{array} $	· · · · · · ·	0 0 0	$= (1) \cdot \det$	0	$egin{array}{c} 0 \ -1 \ 0 \ dots \ 0 \ \ \ 0 \ \ \ \ 0 \ \ 0 \ \ 0 \ \ 0 \ \ \ \ \ 0 \$	-1	•••	0
	[0	0	0		-1]	$= (-1)^{p-2}$					_

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 $F = \mathbf{F}_p$, all eigenvalues/vectors still lie in \mathbf{F}_p , but now -1 = p - 1, making $(x - (p - 1))(x + 1)^{p-1} = (x + 1)(x + 1)^{p-1}$, so $\chi_{A,\mathbf{F}_p}(x) = (x + 1)^p$, and the Jordan blocks may merge.

- A computation shows that $(A+I)^2 = pA = 0 \in M_p(\mathbf{F}_p)$ and $(A+I) \neq 0$, so $\min_{A, \mathbf{F}_p}(x) = (x+1)^2$.
 - Thus the largest Jordan block corresponding to $\lambda = -1$ is of size 2
- Can check that $det(A) = \pm 1 \in \mathbf{F}_p^{\times}$, 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:

$$\min_{A, \mathbf{F}_p} (x) = (x+1)^2$$
$$\chi_{A, \mathbf{F}_p} (x) \equiv (x+1)^p$$
$$\dim E_{-1} = p - 1.$$

Thus

$$JCF_{\mathbf{F}_{p}}(A) = J_{-1}^{2} \oplus (p-2)J_{-1}^{1} = \begin{bmatrix} -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \cdots & -1 & 0 \\ \hline 0 & 0 & 0 & \cdots & -1 & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 & -1 \end{bmatrix}$$

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 \mathbf{F}_p , since

$$\mathbf{v}_1 + \mathbf{p}_1 + \mathbf{p}_2 + \dots + \mathbf{p}_{p-2} = [p - 1, 0, 0, \dots, 0, 1]$$
$$= [-1, 0, 0, \dots, 0, 1]$$
$$= -\mathbf{p}_{p-1}.$$

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 $\mathbf{x} = [1, 0, \dots, 0]$. Thus

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

12.10 Spring 2018 #4

Let

$$A = \begin{bmatrix} 0 & 1 & -2 \\ 1 & 1 & -3 \\ 1 & 2 & -4 \end{bmatrix} \in M_3(\mathbb{C})$$

- a. Find the Jordan canonical form J of A.
- b. Find an invertible matrix P such that $P^{-1}AP = J$.

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

12.11 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 $M_n(\mathbf{C})$?
- b. Find a nonzero matrix $P \in M_n(\mathbf{C})$ such that $P^{-1}AP$ is in Jordan canonical form.

12.12 Spring 2016 #1

Let

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

- a. Find the Jordan canonical form J of A.
- b. Find an invertible matrix P such that $P^{-1}AP = J$. You do not need to compute P^{-1} .

12.13 Spring 2015 #6

Problem 12.13.1 (?) 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.

Solution:

Note that if $\mathbf{x} = [x_1, \dots, x_n]$ then $A\mathbf{x} = [\sum x_i, \sum x_i, \dots, \sum x_i]$, so A acts by summing the entries in \mathbf{x} and setting every coordinate to that sum. By inspection (or clever guessing), we can find eigenvalues and eigenvectors:

• $\lambda = 0$ and:

$$- \mathbf{v}_1 = [1, 0, 0, \cdots, 0, -1]
- \mathbf{v}_2 = [0, 1, 0, \cdots, 0, -1]
- \mathbf{v}_3 = [0, 0, 1, \cdots, 0, -1]
- \cdots
- \mathbf{v}_{n-1} = [0, 0, 0, \cdots, 1, -1]$$

•
$$\lambda = n$$
 and $\mathbf{v}_n = [1, 1, \cdots, 1]$

Note that for $\lambda = n$, we have $A[1, 1, \dots, 1] = [n \cdot 1, \dots, n \cdot 1]$. So for $n \cdot 1 \neq 0$, there are two eigenspaces corresponding to $\lambda = 0, n$, and if $n \cdot 1 = 0$ these collapse to just a single eigenspace for $\lambda = 0$.

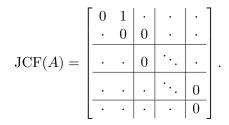
Assuming $n \cdot 1 \neq 0$, we get a characteristic polynomial of $(x - n)x^{n-1}$. The x - n factor corresponds to a single 1×1 Jordan block with diagonal n. For the x^{n-1} factor, we've produced n - 1 distinct eigenvectors, so we get n - 1 Jordan blocks of size 1×1 with diagonal zero. Thus

	\overline{n}	•	•	.	.	
	•	0	•	•	•	
JCF(A) =			0	·	•	
		•	•	·.	•	
	•	•	•	•	0	

One can verify this by checking directly that the minimal polynomial of A is p(x) = (x - n)x, so the size of the largest Jordan block for $\lambda = n$ is 1 and for $\lambda = 0$ is n - 1, while the characteristic polynomial is $(x - n)x^{n-1}$, so the sum of the sizes of Jordan blocks for $\lambda = n$ is 1 and for $\lambda = 0$ is n - 1, forcing the 1×1 blocks everywhere. Now consider the case when $n \cdot 1 = 0$; then \mathbf{v}_n becomes an eigenvector for $\lambda = 0$ instead of $\lambda = n$. The minimal polynomial becomes $(x - 0)x = x^2$ and the characteristic polynomial becomes x^n , so $\lambda = 0$ has:

- The size of the largest Jordan block is 2,
- The sum of sizes of Jordan blocks is n-1,

and so this forces one block of size 2×2 and n-2 blocks of size 1×1 . So we now have:



12.14 Fall 2014 #5

Let T be a 5 × 5 complex matrix with characteristic polynomial $\chi(x) = (x-3)^5$ and minimal polynomial $m(x) = (x-3)^2$. Determine all possible Jordan forms of T.

12.15 Spring 2013 #5

Let $T: V \to V$ be a linear map from a 5-dimensional **C**-vector space to itself and suppose f(T) = 0where $f(x) = x^2 + 2x + 1$.

- 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 $T^2w = w$.
- b. Give all of the possible Jordan canonical forms of T.

12.16 Spring 2021 #1

Let m

$$A \coloneqq \begin{bmatrix} 4 & 1 & -1 \\ -6 & -1 & 2 \\ 2 & 1 & 1 \end{bmatrix} \in \operatorname{Mat}(3 \times 3, \mathbf{C}).$$

- a. Find the Jordan canonical form J of A.
- b. Find an invertible matrix P such that $J = P^{-1}AP$.
- c. Write down the minimal polynomial of A.

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

Concepts Used:

- χ_A(t) = tⁿ tr (Λ¹ A) tⁿ⁻¹ + tr (Λ² A) tⁿ⁻² ··· ± det(A)
 Finding generalized eigenvectors: let B = A λI, get eigenvector v, solve Bw₁ = $v, Bw_2 = w_1, \cdots$ to get a Jordan block. Repeat with any other usual eigenvectors.
- Convention: construct Jordan blocks in decreasing order of magnitude of eigenvalues. ٠
- Polynomial exponent data:
 - Minimal polynomial exponents: sizes of largest Jordan blocks.
 - Characteristic polynomial exponents: sum of sizes of Jordan blocks, i.e. how many times λ is on the diagonal of JCF(A).

Solution:

Proof (parts a and b).

- Write $\chi_A(t) = t^3 T_1 t^2 + T_2 t T_3$ where $T_i \coloneqq \operatorname{tr} \left(\bigwedge^i A \right)$: - $T_1 = \operatorname{tr}(A) = 4 - 1 + 1 = 4.$
 - $-T_2 = (-1-2) + (4+2) + (-4-6) = 5.$ - $T_3 = \det(A) = 4(-1-2) - 1(-10) + (-1)(-6+2) = 2.$
- So $\chi_A(t) = t^3 4t^2 + 5t 2$.
- Try rational roots test: $r \in \{\pm 2/1\}$, and check that 2 is root.
- By polynomial long division, $\chi_A(t)/(t-2) = t^2 2t + 1 = (t-1)^2$.
- So the eigenvalues are $\lambda = 2, 1$.
- $\lambda = 2$:
 - Set $U \coloneqq A \lambda I$, then find RREF(U) to compute its kernel:

	2	1	-1]		2	1	0	
$U\coloneqq$	-6	-3	2	\rightsquigarrow	0	0	1	,
$U \coloneqq$	2	1	-1		0	0	0	

which yields $v_1 = [1, -2, 0]$.

• $\lambda = 2$:

- Similarly,

$$U := \begin{bmatrix} 3 & 1 & -1 \\ -6 & -2 & 2 \\ 2 & 1 & 0 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{bmatrix},$$

which yields
$$v_2 = [1, -2, 1]$$
.

- Solve $Uw = v_3$:

$$\begin{bmatrix} 3 & 1 & -1 & 1 \\ -6 & -2 & 2 & -2 \\ 2 & 1 & 0 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

so take $v_3 = [0, 1, 0]$.

• Putting things together:

$$A = P^{-1}JP \text{ where}$$
$$J = J_1(\lambda = 2) \oplus J_2(\lambda = 1) = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$
$$P = [v_1, v_2, v_3] = \begin{bmatrix} 1 & 1 & 0 \\ -2 & -2 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Proof (part c).

- Write $\min_A(t) = (t-2)(t-1)^{\ell_1}$, then since $\min_A(t)$ divides $\chi_A(t)$ either $\ell_1 = 1, 2$.
- ℓ_1 is the size of the **largest** block corresponding to $\lambda = 1$, which is size 2, so $\lambda_1 = 2$.
- Thus

$$\min_{A}(t) = (t-2)(t-1)^2.$$

12.17 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.

13 Extra Problems

Tons of extra fundamental problems here: https://math.ucr.edu/~mpierce/teaching/ qual-algebra/fun/groups/

(DZG): these are just random extra problems that I found and dropped in. There is likely a ton of overlap/redundancy!

13.1 Linear Algebra

1. For a division ring D, let V_i be a finite dimensional vector space over D for $i \in \{1, \ldots, k\}$. Suppose the sequence

 $0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow \cdots \lor V_k \longrightarrow 0$

is exact. Prove that $\sum_{i=1}^{k} (-1)^i \dim_D V_i = 0.$

- 2. Prove that if A and B are invertible matrices over a field \mathbf{k} , then $A + \lambda B$ is invertible for all but finitely many $\lambda \in \mathbf{k}$.
- 3. For the ring of $n \times n$ matrices over a commutative unital ring R, which we'll denote $\operatorname{Mat}_n(R)$, recall the definition of the determinant map det: $\operatorname{Mat}_n(R) \to R$. For $A \in \operatorname{Mat}_n(R)$ also recall the definition of the classical adjoint A^a of A. Prove that:
- $\det(A^a) = \det(A)^{n-1}$
- $(A^a)^a = \det(A)^{n-2}A$
- 4. If R is an integral domain and A is an $n \times n$ matrix over R, prove that if a system of linear equations Ax = 0 has a nonzero solution then det A = 0. Is the converse true? What if we drop the assumption that R is an integral domain?
- 5. What is the companion matrix M of the polynomial $f = x^2 x + 2$ over C? Prove that f is the minimal polynomial of M.
- 6. Suppose that φ and ψ are commuting endomorphisms of a finite dimensional vector space E over a field \mathbf{k} , so $\varphi \psi = \psi \varphi$.
- Prove that if k is algebraically closed, then φ and ψ have a common eigenvector.
- Prove that if E has a basis consisting of eigenvectors of φ and E has a basis consisting of eigenvectors of ψ , then E has a basis consisting of vectors that are eigenvectors for both φ and ψ simultaneously.

13.2 Galois Theory

Taken from here: https://math.ucr.edu/ ~mpierce/teaching/qual-algebra/fun/ galois/

- 1. Suppose that for an extension field F over K and for $a \in F$, we have that $b \in F$ is algebraic over K(a) but transcendental over K. Prove that a is algebraic over K(b).
- 2. Suppose that for a field F/K that $a \in F$ is algebraic and has odd degree over K. Prove that a^2 is also algebraic and has odd degree over K, and furthermore that $K(a) = K(a^2)$
- 3. For a polynomial $f \in K[x]$, prove that if $r \in F$ is a root of f then for any $\sigma \in \operatorname{Aut}_K F, \sigma(r)$ is also a root of f
- 4. Prove that as extensions of Q, Q(x) is Galois over $Q(x^2)$ but not over $Q(x^3)$.
- 5. If F is over E, and E is over K is F necessarily over K? Answer this question for each of the words "algebraic," "normal," and "separable" in the blanks.

- 6. If F is over K, and E is an intermediate extension of F over K, is F necessarily over E? Answer this question for each of the words "algebraic," "normal," and "separable" in the blanks.
- 7. If F is some (not necessarily Galois) field extension over K such that [F:K] = 6 and Aut ${}_{K}F \simeq S_3$, then F is the splitting field of an irreducible cubic over K[x].
- 8. Recall the definition of the join of two subgroups $H \lor G$ (or H+G). For F a finite dimensional Galois extension over K and let A and B be intermediate extensions. Prove that
- a. $\operatorname{Aut}_{AB} F = \operatorname{Aut}_A F \cap \operatorname{Aut}_B F$
- b. Aut $_{A \cap B}F = \operatorname{Aut}_A F \lor \operatorname{Aut}_B F$
- 9. For a field K take $f \in K[x]$ and let $n = \deg f$. Prove that for a splitting field F of f over K that $[F:K] \leq n!$. Furthermore prove that [F:K] divides n!.
- 10. Let F be the splitting field of $f \in K[x]$ over K. Prove that if $g \in K[x]$ is irreducible and has a root in F, then g splits into linear factors over F.
- 11. Prove that a finite field cannot be algebraically closed.
- 12. For $u = \sqrt{2 + \sqrt{2}}$, What is the Galois group of Q(u) over Q? What are the intermediate fields of the extension Q(u) over Q?
- 13. Characterize the splitting field and all intermediate fields of the polynomial $(x^2 2) (x^2 3) (x^2 5)$ over Q. Using this characterization, find a primitive element of the splitting field.
- 14. Characterize the splitting field and all intermediate fields of the polynomial $x^4 3$ over Q
- 15. Consider the polynomial $f = x^3 x + 1$ in $\mathbf{F}_3[x]$. Prove that f is irreducible. Calculate the degree of the splitting field of f over \mathbf{F}_3 and the cardinality of the splitting field of f.
- 16. Given an example of a finite extension of fields that has infinitely many intermediate fields.
- 17. Let $u = \sqrt{3} + \sqrt{2}$. Is Q(u) a splitting field of u over Q? (MathSE)
- 18. Prove that the multiplicative group of units of a finite field must be cyclic, and so is generated by a single element.
- 19. Prove that \boldsymbol{F}_{p^n} is the splitting field of $x^{p^n} x$ over \boldsymbol{F}_p .
- 20. Prove that for any positive integer n there is an irreducible polynomial of degree n over \mathbf{F}_{p}
- 21. Recall the definition of a perfect field. Give an example of an imperfect field, and the prove that every finite field is perfect.
- 22. For n > 2 let ζ_n denote a primitive n th root of unity over Q. Prove that

$$\left[\boldsymbol{Q}\left(\zeta_n + \zeta_n^{-1} : \boldsymbol{Q}\right)\right] = \frac{1}{2}\varphi(n)$$

where φ is Euler's totient function.

- 23. Suppose that a field K with characteristic not equal to 2 contains an primitive n th root of unity for some odd integer n. Prove that K must also contain a primitive 2n th root of unity.
- 24. Prove that the Galois group of the polynomial $x^n 1$ over Q is abelian.

13.3 Commutative Algebra

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

~

- Show that $\langle 2, x \rangle \leq \mathbf{Z}[x]$ is not a principal ideal.
- Let R be a Noetherian ring and A, B algebras over R. Suppose A is finite type over R and finite over B. Then B is finite type over R.

13.4 Group Theory

13.4.1 Centralizing and Normalizing

- Show that $C_G(H) \subseteq N_G(H) \leq G$.
- Show that $Z(G) \subseteq C_G(H) \subseteq N_G(H)$.
- Given $H \subseteq G$, let $S(H) = \bigcup_{g \in G} gHg^{-1}$, so |S(H)| is the number of conjugates to H. Show that $|S(H)| = [G : N_G(H)]$.
 - That is, the number of subgroups conjugate to ${\cal H}$ equals the index of the normalizer of ${\cal H}.$
- Show that $Z(G) = \bigcap_{a \in G} C_G(a)$.
- Show that the centralizer $G_G(H)$ of a subgroup is again a subgroup.
- Show that $C_G(H) \leq N_G(H)$ is a normal subgroup.
- Show that $C_G(G) = Z(G)$.
- Show that for $H \leq G$, $C_H(x) = H \cap C_G(x)$.
- Let $H, K \leq G$ a finite group, and without using the normalizers of H or K, show that $|HK| = |H||K|/|H \cap K|$.
- Show that if $H \leq N_G(K)$ then $HK \leq H$, and give a counterexample showing that this condition is necessary.
- Show that HK is a subgroup of G iff HK = KH.
- Prove that the kernel of a homomorphism is a normal subgroup.

13.4.2 Primes in Group Theory

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

• Analyze groups of order pq with q < p.

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

- Show that if q does not divide p 1, then G is cyclic.
- Show that G is never simple.
- Analyze groups of order p^2q .

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

- Show that no group of order p^2q^2 is simple for p < q primes.
- Show that a group of order p^2q^2 has a normal Sylow subgroup.
- Show that a group of order p^2q^2 where q does not divide $p^2 1$ and p does not divide $q^2 1$ is abelian.
- Show that every group of order pqr with p < q < r primes contains a normal Sylow subgroup.
 - Show that G is never simple.
- Let p be a prime and $|G| = p^3$. Prove that G has a normal subgroup N of order p^2 .
 - Suppose $N = \langle h \rangle$ is cyclic and classify all possibilities for G if: $\Diamond |h| = p^{3}$ $\Diamond |h| = p.$

Hint: Sylow and semidirect products.

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

13.4.3 p-Groups

- Show that every *p*-group has a nontrivial center.
- Show that every *p*-group is nilpotent.
- Show that every *p*-group is solvable.
- Show that every maximal subgroup of a *p*-group has index *p*.

- Show that every maximal subgroup of a *p*-group is normal.
- Show that every group of order p is cyclic.
- Show that every group of order p^2 is abelian and classify them.
- Show that every normal subgroup of a *p*-group is contained in the center.

Hint: Consider G/Z(G).

- Let $O_P(G)$ be the intersection of all Sylow *p*-subgroups of *G*. Show that $O_p(G) \leq G$, is maximal among all normal *p*-subgroups of *G*
- Let $P \in \operatorname{Syl}_{p}(H)$ where $H \leq G$ and show that $P \cap H \in \operatorname{Syl}_{p}(H)$.
- Show that Sylow p_i -subgroups S_{p_1}, S_{p_2} for distinct primes $p_1 \neq p_2$ intersect trivially.
- Show that in a *p* group, every normal subgroup intersects the center nontrivially.

13.4.4 Symmetric Groups

Specific Groups

- Show that the center of S_3 is trivial.
- Show that $Z(S_n) = 1$ for $n \ge 3$
- Show that $\operatorname{Aut}(S_3) = \operatorname{Inn}(S_3) \cong S_3$.
- Show that the transitive subgroups of S_3 are S_3, A_3
- Show that the transitive subgroups of S_4 are $S_4, A_4, D_4, \mathbf{Z}_2^2, \mathbf{Z}_4$.
- Show that S_4 has two normal subgroups: A_4, \mathbf{Z}_2^2 .
- Show that $S_{n\geq 5}$ has one normal subgroup: A_n .
- $Z(A_n) = 1$ for $n \ge 4$
- Show that $[S_n, S_n] = A_n$
- Show that $[A_4, A_4] \cong \mathbb{Z}_2^2$
- Show that $[A_n, A_n] = A_n$ for $n \ge 5$, so $A_{n>5}$ is nonabelian.

General Structure

- Show that an m-cycle is an odd permutation iff m is an even number.
- Show that a permutation is odd iff it has an odd number of even cycles.
- Show that the center of S_n for $n \ge 4$ is nontrivial.
- Show that disjoint cycles commute.
- Show directly that any k-cycle is a product of transpositions, and determine how many transpositions are needed.

Generating Sets

13.4 Group Theory

Group	Generating Set	Size	Γ
$S_n, n \ge 2$	(<i>ij</i>)'s	$\frac{n(n-1)}{2}$	Γ
	$(12), (13), \ldots, (1n)$	n-1	
	$(12), (23), \ldots, (n-1 n)$	n-1	
	$(12), (12n)$ if $n \ge 3$	2	
	$(12), (23n)$ if $n \ge 3$	2	!
	(ab), (12n) if $(b-a, n) = 1$	2	
$A_n, n \ge 3$	3-cycles	$\frac{n(n-1)(n-2)}{3}$	Γ
	(1 <i>ij</i>)'s	(n-1)(n-2)	
	(12 <i>i</i>)'s	n-2	
	$(i \ i + 1 \ i + 2)$'s	n-2	
	$(123), (12n)$ if $n \ge 4$ odd	2	
	$(123), (23n)$ if $n \ge 4$ even	2	L

• Show that S_n is generated by any of the following types of cycles:

- Show that S_n is generated by transpositions.
- Show that S_n is generated by *adjacent* transpositions.
- Show that S_n is generated by $\{(12), (12 \cdots n)\}$ for $n \ge 2$
- Show that S_n is generated by $\{(12), (23 \cdots n)\}$ for $n \ge 3$
- Show that S_n is generated by $\{(ab), (12 \cdots n)\}$ where $1 \le a < b \le n$ iff gcd(b-a, n) = 1.
- Show that S_p is generated by any arbitrary transposition and any arbitrary *p*-cycle.

13.4.5 Alternating Groups

- Show that A_n is generated 3-cycles.
- Prove that A_n is normal in S_n .
- Argue that A_n is simple for $n \ge 5$.
- Show that $Out(A_4)$ is nontrivial.

13.4.6 Dihedral Groups

• Show that if $N \leq D_n$ is a normal subgroup of a dihedral group, then D_n/N is again a dihedral group.

13.4.7 Other Groups

- Show that **Q** is not finitely generated as a group.
- Show that the Quaternion group has only one element of order 2, namely -1.

13.4.8 Classification

- Show that no group of order 36 is simple.
- Show that no group of order 90 is simple.
- Classifying all groups of order 99.
- Show that all groups of order 45 are abelian.
- Classify all groups of order 10.
- Classify the five groups of order 12.
- Classify the four groups of order 28.
- Show that if |G| = 12 and has a normal subgroup of order 4, then $G \cong A_4$.
- Suppose $|G| = 240 = s^4 \cdot 3 \cdot 5$.
 - How many Sylow-p subgroups does G have for $p \in \{2, 3, 5\}$?
 - Show that if G has a subgroup of order 15, it has an element of order 15.
 - Show that if G does not have such a subgroup, the number of Sylow-3 subgroups is either 10 or 40.

Hint: Sylow on the subgroup of order 15 and semidirect products.

13.4.9 Group Actions

- Show that the stabilizer of an element G_x is a subgroup of G.
- Show that if x, y are in the same orbit, then their stabilizers are conjugate.
- Show that the stabilizer of an element need not be a normal subgroup?
- Show that if $G \curvearrowright X$ is a group action, then the stabilizer G_x of a point is a subgroup.

13.4.10 Series of Groups

- Show that A_n is simple for $n \ge 5$
- Give a necessary and sufficient condition for a cyclic group to be solvable.
- Prove that every simple abelian group is cyclic.
- Show that S_n is generated by disjoint cycles.
- Show that S_n is generated by transpositions.

- Show if G is finite, then G is solvable \iff all of its composition factors are of prime order.
- Show that if N and G/N are solvable, then G is solvable.
- Show that if G is finite and solvable then every composition factor has prime order.
- Show that G is solvable iff its derived series terminates.
- Show that S_3 is not nilpotent.
- Show that G nilpotent $\implies G$ solvable
- Show that nilpotent groups have nontrivial centers.
- Show that Abelian \implies nilpotent
- Show that p-groups \implies nilpotent

13.4.11 Misc

- Prove Burnside's theorem.
- Show that $\operatorname{Inn}(G) \trianglelefteq Aut(G)$
- Show that $\operatorname{Inn}(G) \cong G/Z(G)$
- Show that the kernel of the map $G \to \operatorname{Aut}(G)$ given by $g \mapsto (h \mapsto ghg^{-1})$ is Z(G).
- Show that $N_G(H)/C_G(H) \cong A \leq Aut(H)$
- Give an example showing that normality is not transitive: i.e. $H \trianglelefteq K \trianglelefteq G$ with H not normal in G.

13.4.12 Nonstandard Topics

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

 $Thus \ ``characteristic" is \ a \ strictly \ stronger \ condition \\ than \ normality$

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

So "characteristic" is a transitive relation for subgroups. • Show that if $H \leq G$, $K \leq G$ is a normal subgroup, and H char K then H is normal in G.

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

13.5 Ring Theory

13.5.1 Basic Structure

- Show that if an ideal $I \leq R$ contains a unit then I = R.
- Show that R^{\times} need not be closed under addition.

13.5.2 Ideals

• \star Show that if x is not a unit, then x is contained in some maximal ideal.

Problem 13.5.1 (Units or Zero Divisors) Every $a \in R$ for a finite ring is either a unit or a zero divisor.

Solution:

- Let $a \in R$ and define $\varphi(x) = ax$.
- If φ is injective, then it is surjective, so 1 = ax for some $x \implies x^{-1} = a$.
- Otherwise, $ax_1 = ax_2$ with $x_1 \neq x_2 \implies a(x_1 x_2) = 0$ and $x_1 x_2 \neq 0$
- So *a* is a zero divisor.

Problem 13.5.2 (Maximal implies prime) Maximal \implies prime, but generally not the converse.

Solution: • Suppose \mathfrak{m} is maximal, $ab \in \mathfrak{m}$, and $b \notin \mathfrak{m}$.

- Then there is a containment of ideals $\mathfrak{m} \subsetneq \mathfrak{m} + (b) \Longrightarrow \mathfrak{m} + (b) = R$.
- So

$$1 = m + rb \implies a = am + r(ab),$$

but $am \in \mathfrak{m}$ and $ab \in \mathfrak{m} \implies a \in \mathfrak{m}$. Counterexample: $(0) \in \mathbb{Z}$ is prime since \mathbb{Z} is a domain, but not maximal since it is properly contained in any other ideal.

- Show that every proper ideal is contained in a maximal ideal
- Show that if $x \in R$ a PID, then x is irreducible $\iff \langle x \rangle \trianglelefteq R$ is maximal.
- Show that intersections, products, and sums of ideals are ideals.
- Show that the union of two ideals need not be an ideal.
- Show that every ring has a proper maximal ideal.
- Show that $I \leq R$ is maximal iff R/I is a field.
- Show that $I \leq R$ is prime iff R/I is an integral domain.
- Show that $\cup_{\mathfrak{m}\in \max \operatorname{Spec}(R)} = R \setminus R^{\times}$.
- Show that $\max \operatorname{Spec}(R) \subsetneq \operatorname{Spec}(R)$ but the containment is strict.
- Show that every prime ideal is radical.
- Show that the nilradical is given by $\sqrt{0_R} = \sqrt{(0)}$.
- Show that $rad(IJ) = rad(I) \cap rad(J)$
- Show that if $\operatorname{Spec}(R) \subseteq \max\operatorname{Spec}(R)$ then R is a UFD.
- Show that if R is Noetherian then every ideal is finitely generated.

13.5.3 Characterizing Certain Ideals

- Show that for an ideal $I \leq R$, its radical is the intersection of all prime ideals containing I.
- Show that \sqrt{I} is the intersection of all prime ideals containing *I*.

Problem 13.5.3 (Jacobson radical is bigger than the nilradical) The nilradical is contained in the Jacobson radical, i.e.

$$\sqrt{0_R} \subseteq J(R).$$

Solution:

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

Problem 13.5.4 (Mod by nilradical to kill nilpotents) $R/\sqrt{0_R}$ has no nonzero nilpotent elements.

Solution:

$$a + \sqrt{0_R} \text{ nilpotent} \implies (a + \sqrt{0_R})^n \coloneqq a^n + \sqrt{0_R} = \sqrt{0_R}$$
$$\implies a^n \in \sqrt{0_R}$$
$$\implies \exists \ell \text{ such that } (a^n)^\ell = 0$$
$$\implies a \in \sqrt{0_R}.$$

Problem 13.5.5 (Nilradical is intersection of primes) The nilradical is the intersection of all prime ideals, i.e.

$$\sqrt{0_R} = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}$$

Solution:

- $\sqrt{0_R} \subseteq \cap \mathfrak{p}$:
- $x \in \sqrt{0_R} \implies x^n = 0 \in \mathfrak{p} \implies x \in \mathfrak{p} \text{ or } x^{n-1} \in \mathfrak{p}.$
- $R \setminus \sqrt{0_R} \subseteq \cup_{\mathfrak{p}}(R \setminus \mathfrak{p})$:
- Define $S = \{ I \leq R \mid a^n \notin I \text{ for any } n \}.$
- Then apply Zorn's lemma to get a maximal ideal \mathfrak{m} , and maximal \implies prime.

13.5.4 Misc

- Show that localizing a ring at a prime ideal produces a local ring.
- Show that R is a local ring iff for every $x \in R$, either x or 1 x is a unit.
- Show that if R is a local ring then $R \setminus R^{\times}$ is a proper ideal that is contained in the Jacobson radical J(R).
- Show that if $R \neq 0$ is a ring in which every non-unit is nilpotent then R is local.
- Show that every prime ideal is primary.
- Show that every prime ideal is irreducible.

13.6 Field Theory

General Algebra

- Show that any finite integral domain is a field.
- Show that every field is simple.
- Show that any field morphism is either 0 or injective.
- Show that if L/F and α is algebraic over both F and L, then the minimal polynomial of α over L divides the minimal polynomial over F.
- Prove that if R is an integral domain, then R[t] is again an integral domain.
- Show that ff(R[t]) = ff(R)(t).
- Show that $[\mathbf{Q}(\sqrt{2} + \sqrt{3}) : \mathbf{Q}] = 4.$
 - Show that $\mathbf{Q}(\sqrt{2} + \sqrt{3}) = \mathbf{Q}(\sqrt{2} \sqrt{3}) = \mathbf{Q}(\sqrt{2}, \sqrt{3}).$
- Show that the splitting field of $f(x) = x^3 2$ is $\mathbf{Q}(\sqrt[3]{2}, \zeta_2)$.

13

Extensions?

- What is $[\mathbf{Q}(\sqrt{2} + \sqrt{3}) : \mathbf{Q}]$?
- What is $[\mathbf{Q}(2^{\frac{3}{2}}):\mathbf{Q}]$?
- Show that if $p \in \mathbf{Q}[x]$ and $r \in \mathbf{Q}$ is a rational root, then in fact $r \in \mathbf{Z}$.
- If $\{\alpha_i\}_{i=1}^n \subset F$ are algebraic over K, show that $K[\alpha_1, \cdots, \alpha_n] = K(\alpha_1, \cdots, \alpha_n)$.
- Show that α/F is algebraic $\iff F(\alpha)/F$ is a finite extension.
- Show that every finite field extension is algebraic.
- Show that if α, β are algebraic over F, then $\alpha \pm \beta, \alpha \beta^{\pm 1}$ are all algebraic over F.
- Show that if L/K/F with K/F algebraic and L/K algebraic then L is algebraic.

Special Polynomials

- Show that a field with p^n elements has exactly one subfield of size p^d for every d dividing n.
- Show that $x^{p^n} x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n.
- Show that $x^{p^d} x \mid x^{p^n} x \iff d \mid n$
- Prove that $x^{p^n} x$ is the product of all monic irreducible polynomials in $\mathbf{F}_p[x]$ with degree dividing n.
- Prove that an irreducible $\pi(x) \in \mathbf{F}_p[x]$ divides $x^{p^n} x \iff \deg \pi(x)$ divides n.

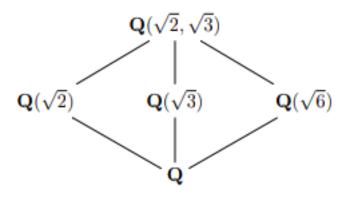
13.7 Galois Theory

13.7.1 Theory

- Show that if K/F is the splitting field of a separable polynomial then it is Galois.
- Show that any quadratic extension of a field F with $ch(F) \neq 2$ is Galois.
- Show that if K/E/F with K/F Galois then K/E is always Galois with $g(K/E) \leq g(K/F)$.
 - Show additionally E/F is Galois $\iff g(K/E) \trianglelefteq g(K/F)$.
 - Show that in this case, g(E/F) = g(K/F)/g(K/E).
- Show that if E/k, F/k are Galois with $E \cap F = k$, then EF/k is Galois and $G(EF/k) \cong G(E/k) \times G(F/k)$.

13.7.2 Computations

- Show that the Galois group of $x^n 2$ is D_n , the dihedral group on n vertices.
- Compute all intermediate field extensions of $\mathbf{Q}(\sqrt{2},\sqrt{3})$, show it is equal to $\mathbf{Q}(\sqrt{2}+\sqrt{3})$, and find a corresponding minimal polynomial.



- Compute all intermediate field extensions of $\mathbf{Q}(2^{\frac{1}{4}}, \zeta_8)$.
- Show that $\mathbf{Q}(2^{\frac{1}{3}})$ and $\mathbf{Q}(\zeta_3 2^{\frac{1}{3}})$
- Show that if L/K is separable, then L is normal \iff there exists a polynomial $p(x) = \prod_{i=1}^{n} x \alpha_i \in K[x]$ such that $L = K(\alpha_1, \cdots, \alpha_n)$ (so L is the splitting field of p).
- Is $\mathbf{Q}(2^{\frac{1}{3}})/\mathbf{Q}$ normal?
- Show that $\mathbf{GF}(p^n)$ is the splitting field of $x^{p^n} x \in \mathbf{F}_p[x]$.
- Show that $\mathbf{GF}(p^d) \leq \mathbf{GF}(p^n) \iff d \mid n$
- Compute the Galois group of $x^n 1 \in \mathbf{Q}[x]$ as a function of n.
- Identify all of the elements of the Galois group of $x^p 2$ for p an odd prime (note: this has a complicated presentation).
- Show that $\operatorname{Gal}(x^{15}+2)/\mathbf{Q} \cong S_2 \rtimes \mathbf{Z}/15\mathbf{Z}$ for S_2 a Sylow 2-subgroup.
- Show that $\operatorname{Gal}(x^3 + 4x + 2)/\mathbf{Q} \cong S_3$, a symmetric group.

13.8 Modules and Linear Algebra

- Prove the Cayley-Hamilton theorem.
- Prove that the minimal polynomial divides the characteristic polynomial.
- Prove that the cokernel of $A \in Mat(n \times n, \mathbb{Z})$ is finite $\iff \det A \neq 0$, and show that in this case |coker(A)| = |det(A)|.
- Show that a nilpotent operator is diagonalizable.
- Show that if A, B are diagonalizable and [A, B] = 0 then A, B are simultaneously diagonalizable.
- Does diagonalizable imply invertible? The converse?
- Does diagonalizable imply distinct eigenvalues?
- Show that if a matrix is diagonalizable, its minimal polynomial is squarefree.
- Show that a matrix representing a linear map $T: V \to V$ is diagonalizable iff V is a direct sum of eigenspaces $V = \bigoplus_i \ker(T \lambda_i I)$.
- Show that if $\{\mathbf{v}_i\}$ is a basis for V where dim(V) = n and $T(\mathbf{v}_i) = \mathbf{v}_{i+1 \mod n}$ then T is diagonalizable with minimal polynomial $x^n 1$.
- Show that if the minimal polynomial of a linear map T is irreducible, then every T-invariant subspace has a T-invariant complement.

13.9 Linear Algebra

Sort out from module section.

14 Even More Algebra Questions

Remark 14.0.1: (DZG): These all come from a random PDF I found, but I couldn't find the original author/source!

14.1 Groups

14.1.1 Question 1.1

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

14.1.2 Question 1.2

Prove that a subgroup of index two is normal.

14.1.3 Question 1.3

Find all normal subgroups of A_4 .

14.1.4 Question 1.4

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

14.1.5 Question 1.5

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

14.1.6 Question 1.6.

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

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

14.1.7 Question 1.7

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

14.1.8 Question 1.8

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

14.1.9 Question 1.9

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

14.1.10 Question 1.10

What are all possible orders of elements of $SL_2(Z)$?

14.1.11 Question 1.11

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

14.1.12 Question 1.12

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

14.1.13 Question 1.13

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

14.1.14 Question 1.14

Give examples of simple groups. Are there infinitely many?

14.1.15 Question 1.15

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

14.1.16 Question 1.16

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

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

14.1.17 Question 1.17

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

14.1.18 Question 1.18

Talk about conjugacy classes in the symmetric group S_n .

14.1.19 Question 1.19

When do conjugacy classes in S_n split in A_n ?

14.1.20 Question 1.20

What is the centre of S_n ? Prove it.

14.1.21 Question 1.21

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

14.1.22 Question 1.22

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

14.1.23 Question 1.23

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

14.1.24 Question 1.24

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

14.1.25 Question 1.25

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

14.1.26 Question 1.26.

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

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

Do you know the classification of higher-dimensional polyhedra?

14.1.27 Question 1.27

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

14.1.28 Question 1.28

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

14.1.29 Question 1.29

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

14.1.30 Question 1.30

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

14.1.31 Question 1.31

Consider $SL_2(R)$ acting on \mathbb{R}^2 by matrix multiplication. What is the stabiliser of a point? Does it depend which point? Do you know what sort of subgroup this is? What if $SL_2(R)$ acts by Möbius transformations instead?

14.1.32 Question 1.32

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

14.1.33 Question 1.33

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

14.1.34 Question 1.34

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

14.1.35 Question 1.35

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

14.1.36 Question 1.36

What groups have nontrivial automorphisms?

14.1.37 Question 1.37

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

14.1.38 Question 1.38

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

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

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

14.1.39 Question 1.39

Let's look at $SL_2(\mathbf{F}_3)$. How many elements are in that group? What is its centre? Identify $PSL_2(\mathbf{F}_3)$ as a permutation group.

14.1.40 Question 1.40

How many elements does $\mathfrak{gl}_2(\mathbf{F}_q)$ have? How would you construct representations?

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

14.1.41 Question 1.41.

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

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

14.1.42 Question 1.42

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

14.1.43 Question 1.43

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

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

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

14.1.44 Question 1.44

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

~

14.2 Classification of Finite groups

14.2.1 Question 2.1

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

14.2.2 Question 2.2

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

14.2.3 Question 2.3

State/prove the Sylow theorems.

14.2.4 Question 2.4

Classify groups of order 35.

14

14.2.5 Question 2.5

Classify groups of order 21.

14.2.6 Question 2.6

Discuss groups of order 55.

14.2.7 Question 2.7

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

14.2.8 Question 2.8

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

14.2.9 Question 2.9

Classify all groups of order 8.

14.2.10 Question 2.10

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

14.2.11 Question 2.11

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

14.2.12 Question 2.12

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

14.2.13 Question 2.13

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

14.2.14 Question 2.14

How many abelian groups are there of order 36?

14.2.15 Question 2.15

What are the abelian groups of order 16?

14.2.16 Question 2.16.

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

14.2.17 Question 2.17

How many abelian groups of order 200 are there?

14.2.18 Question 2.18

Prove there is no simple group of order 132.

14.2.19 Question 2.19

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

14.2.20 Question 2.20

Prove that there is no simple group of order 40.

14.3 Fields and Galois Theory

14.3.1 Question 3.1

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

14.3.2 Question 3.2

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

14.3.3 Question 3.3

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

14.3.4 Question 3.4

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

14.3.5 Question 3.5

What's the field with 25 elements?

14.3.6 Question 3.6

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

14.3.7 Question 3.7

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

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

14.3.8 Question 3.8

Are there separable polynomials of any degree over any field?

14.3.9 Question 3.9

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

14.3.10 Question 3.10

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

14.3.11 Question 3.11

What is a Galois extension?

14.3.12 Question 3.12

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

14.3.13 Question 3.13.

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

14.3.14 Question 3.14

What is a Kummer extension?

14.3.15 Question 3.15

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

14.3.16 Question 3.16

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

14.3.17 Question 3.17

What is the discriminant of a polynomial?

14.3.18 Question 3.18

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

14.3.19 Question 3.19

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

14.3.20 Question 3.20

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

14.3.21 Question 3.21

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

14.3.22 Question 3.22

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

14.3.23 Question 3.23

What is the Galois group of

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

14.3.24 Question 3.24

What is the Galois group of

$$\mathbf{Q}(\sqrt{n_1},\cdots,\sqrt{n_m}) / \mathbf{Q}(\sqrt{n_1}+\cdots+\sqrt{n_m})?$$

14.3.25 Question 3.25

What are the Galois groups of irreducible cubics?

14.3.26 Question 3.26

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

14.3.27 Question 3.27

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

14.3.28 Question 3.28

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

14.3.29 Question 3.29

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

14.3.30 Question 3.30

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

14.3.31 Question 3.31

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

14.3.32 Question 3.32

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

14.3.33 Question 3.33

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

14.3.34 Question 3.34.

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

14.3.35 Question 3.35

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

14.3.36 Question 3.36

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

14.3.37 Question 3.37

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

14.3.38 Question 3.38

What is the Galois group of the polynomial $x^n - 1$ over **Q**?

14.3.39 Question 3.39

Describe the Galois theory of cyclotomic extensions.

14.3.40 Question 3.40

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

14.3.41 Question 3.41

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

14.3.42 Question 3.42

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

14.3.43 Question 3.43

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

14.3.44 Question 3.44

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

14.3.45 Question 3.45

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

14.3.46 Question 3.46

Give a polynomial with S_3 as its Galois group.

14.3.47 Question 3.47

Give an example of a cubic with Galois group S_3 .

14.3.48 Question 3.48

How do you construct a polynomial over **Q** whose Galois group is S_n ? Do it for n = 7 in particular.

14.3.49 Question 3.49

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

14.3.50 Question 3.50

Which finite groups are Galois groups for some field extension?

14.3.51 Question 3.51

What Galois group would you expect a cubic to have?

14.3.52 Question 3.52

Draw the subgroup lattice for S_3 .

14.3.53 Question 3.53

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

14.3.54 Question 3.54

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

14.3.55 Question 3.55

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

14.3.56 Question 3.56.

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

14.3.57 Question 3.57

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

14.3.58 Question 3.58

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

14.3.59 Question 3.59

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

14.3.60 Question 3.60

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

14.3.61 Question 3.61

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

14.3.62 Question 3.62

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

14.3.63 Question 3.63

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

14.3.64 Question 3.64

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

14.3.65 Question 3.65

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

14.3.66 Question 3.66

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

14.3.67 Question 3.67

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

14.3.68 Question 3.68

State and prove Eisenstein's Criterion.

14.3.69 Question 3.69

Why is $(x^p - 1)/(x - 1)$ irreducible over **Q**?

14.3.70 Question 3.70

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

14.3.71 Question 3.71

What are the symmetric polynomials?

14.3.72 Question 3.72

State the fundamental theorem of symmetric polynomials.

14.3.73 Question 3.73

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

14.3.74 Question 3.74

Find a non-symmetric polynomial whose square is symmetric.

14.3.75 Question 3.75

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

14.3.76 Question 3.76

Define p-adic numbers. What is a valuation?

14.3.77 Question 3.77

What's Hilbert's theorem 90?

14.3.78 Question 3.78

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

14.4 Normal Forms

14.4.1 Question 4.1

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

14.4.2 Question 4.2

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

14.4.3 Question 4.3

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

14.4.4 Question 4.4

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

14.4.5 Question 4.5

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

14.4.6 Question 4.6

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

~

14.4.7 Question 4.7

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

14.4.8 Question 4.8

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

14.4.9 Question 4.9

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

14.4.10 Question 4.10

What is rational canonical form?

14.4.11 Question 4.11

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

14.4.12 Question 4.12

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

14.4.13 Question 4.13

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

14.4.14 Question 4.14

What is a nilpotent matrix?

14.4.15 Question 4.15

When do the powers of a matrix tend to zero?

14.4.16 Question 4.16

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

14.4.17 Question 4.17

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

14.4.18 Question 4.18

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

14.4.19 Question 4.19

Is a square matrix always similar to its transpose?

14.4.20 Question 4.20

What are the conjugacy classes of $SL_2(\mathbf{R})$?

14.4.21 Question 4.21

What are the conjugacy classes in $GL_2(\mathbf{C})$?

14.5 Matrices and Linear Algebra

14.5.1 Question 5.1

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

14.5.2 Question 5.2

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

14.5.3 Question 5.3

Explain geometrically how you diagonalise a quadratic form.

14.5.4 Question 5.4

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

14.5.5 Question 5.5

Classify real division algebras.

14.5.6 Question 5.6

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

14.5.7 Question 5.7

Do you know about singular value decomposition?

~

14.5.8 Question 5.8

What are the eigenvalues of a symmetric matrix?

14.5.9 Question 5.9

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

14.5.10 Question 5.10

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

14.5.11 Question 5.11

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

14.5.12 Question 5.12

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

14.5.13 Question 5.13

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

14.5.14 Question 5.14

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

14.5.15 Question 5.15

State/prove the Cayley–Hamilton theorem.

14.5.16 Question 5.16

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

14.5.17 Question 5.17

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

14.5.18 Question 5.18

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

14.5.19 Question 5.19

What is a Toeplitz operator?

14.5.20 Question 5.20

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

 \sim

14.6 Rings

14.6.1 Question 6.1

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

14.6.2 Question 6.2

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

14.6.3 Question 6.3

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

14.6.4 Question 6.4

Do polynomials in several variables form a PID?

14.6.5 Question 6.5

Prove that the integers form a PID.

14.6.6 Question 6.6

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

14.6.7 Question 6.7

What is the relation between Euclidean domains and PIDs?

14.6.8 Question 6.8

Do you know a PID that's not Euclidean?

14.6.9 Question 6.9

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

14.6.10 Question 6.10

Is a ring of formal power series a UFD?

14.6.11 Question 6.11

Is a polynomial ring over a UFD again a UFD?

14.6.12 Question 6.12

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

14.6.13 Question 6.13

Give an example of a ring where unique factorisation fails.

14.6.14 Question 6.14

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

14.6.15 Question 6.15

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

14.6.16 Question 6.16

Find all primes in the ring of Gaussian integers.

14.6.17 Question 6.17

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

14.6.18 Question 6.18

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

14.6.19 Question 6.19

Do you know about Dedekind domains and class numbers?

14.6.20 Question 6.20

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

14.6.21 Question 6.21

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

14.6.22 Question 6.22

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

14.6.23 Question 6.23.

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

14.6.24 Question 6.24

What are the radical ideals in \mathbf{Z} ?

14.6.25 Question 6.25

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

14.6.26 Question 6.26

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

14.6.27 Question 6.27

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

14.6.28 Question 6.28

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

14.6.29 Question 6.29

Is the following map an isomorphism?

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

14.6.30 Question 6.30

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

14.6.31 Question 6.31

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

14.6.32 Question 6.32

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

14.6.33 Question 6.33

Define "Noetherian ring". give an example.

14.6.34 Question 6.34

Prove the Hilbert basis theorem.

14.6.35 Question 6.35

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

14.6.36 Question 6.36

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

14.6.37 Question 6.37

Give an example of an Artinian ring.

14.6.38 Question 6.38

State the structure theorem for semisimple Artinian rings.

14.6.39 Question 6.39

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

14.6.40 Question 6.40

What is a matrix algebra?

14.6.41 Question 6.41

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

14.6.42 Question 6.42.

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

14.6.43 Question 6.43

State the structure theorem for simple rings.

14.6.44 Question 6.44

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

14.6.45 Question 6.45

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

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

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

14.6.46 Question 6.46

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

14.6.47 Question 6.47

Prove that all finite integral domains are fields.

14.6.48 Question 6.48

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

14.6.49 Question 6.49

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

14.6.50 Question 6.50

Give an example of a **C**-algebra which is not semisimple.

14.6.51 Question 6.51

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

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

14.6.52 Question 6.52

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

14.7 Modules

14.7.1 Question 7.1

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

14.7.2 Question 7.2

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

14.7.3 Question 7.3

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

Does D have to be a PID?

14.7.4 Question 7.4

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

14.7.5 Question 7.5

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

14.7.6 Question 7.6.

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

14.7.7 Question 7.7

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

14.7.8 Question 7.8

What is a projective module?

14.7.9 Question 7.9

What is an injective module?

14.7.10 Question 7.10

Do you know an example of a flat module?

14.8 Representation Theory

14.8.1 Question 8.1

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

14.8.2 Question 8.2

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

14.8.3 Question 8.3

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

14.8.4 Question 8.4

State/prove/explain Schur's lemma.

14.8.5 Question 8.5

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

14.8.6 Question 8.6

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

14.8.7 Question 8.7

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

~

14.8.8 Question 8.8

Why is the character table a square?

14.8.9 Question 8.9

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

14.8.10 Question 8.10

What's the regular representation?

14.8.11 Question 8.11

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

14.8.12 Question 8.12

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

14.8.13 Question 8.13

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

14.8.14 Question 8.14.

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

14.8.15 Question 8.15

What is Frobenius reciprocity?

14.8.16 Question 8.16

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

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

14.8.17 Question 8.17

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

14.8.18 Question 8.18

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

Is it possible to work over other fields?

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

14.8.19 Question 8.19

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

14.8.20 Question 8.20

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

14.8.21 Question 8.21

What are the irreducible representations of finite abelian groups?

14.8.22 Question 8.22

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

14.8.23 Question 8.23

Are there two nonisomorphic groups with the same representations?

14.8.24 Question 8.24

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

14.8.25 Question 8.25

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

14.8.26 Question 8.26

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

14.8.27 Question 8.27

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

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

14.8.28 Question 8.28

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

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

14.8.29 Question 8.29

Write the character table for S_4 .

14.8.30 Question 8.30

Start constructing the character table for S_5 .

14.8.31 Question 8.31.

How many irreducible representations does S_n have?

What classical function in mathematics does this number relate to?

14.8.32 Question 8.32

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

14.8.33 Question 8.33

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

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

Which are the indecomposable modules?

14.8.34 Question 8.34

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

14.8.35 Question 8.35

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

14.8.36 Question 8.36

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

14.8.37 Question 8.37

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

14.9 Categories and Functors

14.9.1 Question 9.1

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

14.9.2 Question 9.2

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

14.9.3 Question 9.3

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