Qual Algebra

Table of Contents

Contents

1 Preface

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

- Paco Adajar
- Swaroop Hegde

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

2 Group Theory: General

2.1 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.,

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

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 $\{1, \dots, n\}$. Suppose that $g \in S_n$ sends i to g_i for $i = 1, \dots, n$. Let (a, b) denote as usual the cycle notation for the transposition which permutes a and b. For $i \in \{1, \dots, n-1\}$, compute $\varphi_g((i, i+1))$.

d. Suppose that an automorphism $\varphi \in \operatorname{Aut}(S_n)$ 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.

Concept review omitted.

Strategy omitted.

Solution omitted.

2.2.2 Fall 2014 #6

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

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

Concept review omitted.

Strategy omitted.

Solution omitted.

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.

Solution omitted.

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.

Concept review omitted.

Strategy omitted.

Solution omitted.

2.4 Group Actions / Representations

2.4.1 Spring 2017 #1

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

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

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

⚠**Warning 2.4.1**
(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.

Concept review omitted.

Solution omitted.

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.

Solution omitted.

2.5 Conjugacy Classes

2.5.1 Spring 2021 #2

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

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

Concept review omitted.

Strategy omitted.

Proof omitted.

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.

Concept review omitted.

Solution omitted.

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.

Solution omitted.

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.

Concept review omitted.

Solution omitted.

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.

Concept review omitted.

Strategy omitted.

Solution omitted.

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

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

Solution omitted.

2.6.5 Fall 2019 Midterm #1

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

Solution omitted.

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

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

3.2 Fall 2015 #2

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

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

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

3.3 Spring 2016 #5

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

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

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

3.4 Fall 2017 #1

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

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

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

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

3.5 Fall 2018 #2

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

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

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

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

Concept review omitted.

Solution omitted.

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.

Concept review omitted.

Solution omitted.

4.2 Fall 2019 Midterm #2

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

4.3 Fall 2013 #2

Let G be a group of order 30.

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

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

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

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

4.4 Spring 2014 #2

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

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

b. Show that H is normal in G.

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

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

4.5 Fall 2014 #2

Let G be a group of order 96.

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

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

4.6 Spring 2016 #3

a. State the three Sylow theorems.

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

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

4.7 Spring 2017 #2

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

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

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

4.8 Fall 2017 #2

a. Classify the abelian groups of order 36.

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

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

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

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

4.9 Fall 2012 #2

Let G be a group of order 30.

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

b. Give all possible presentations and relations for G.

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

4.10 Fall 2018 #1

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

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

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

Concept review omitted.

Solution omitted.

4.11 Fall 2019 #2

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

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

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

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

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

Concept review omitted.

Solution omitted.

4.12 Spring 2021 #3

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

b. State the 3 Sylow theorems.

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

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

4.13 Fall 2020 #1

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

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

4.14 Fall 2020 #2

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

a. Prove that G is solvable.

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

5 | Groups: Classification

5.1 Spring 2020 #1

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

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

c. Describe one nonabelian group of order 2020.

Work this problem.

5.2 Spring 2019 #3

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

Describe a representative from each class.

Concept review omitted.

Solution omitted.

Revisit, seems short.

5.3 Spring 2012 #3

Let G be a group of order 70.

a. Show that G is not simple.

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

5.4 Fall 2016 #3

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

5.5 Spring 2018 #1

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

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

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

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

Concept review omitted.

Solution omitted.

6 | Groups: Simple and Solvable

6.1 $\star$ Fall 2016 #7

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

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

Hint: you can use that S_4 is solvable.

6.2 Spring 2015 #4

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

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

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

is an injective homomorphism.

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

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

Hint: use part (b).

6.3 Spring 2014 #1

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

6.4 Fall 2013 #1

Let p, q be distinct primes.

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

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

6.5 Spring 2013 #4

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

6.6 Fall 2019 Midterm #3

Show that there exist no simple groups of order 148.

7 | Commutative Algebra

7.1 UFDs, PIDs, etc

7.1.1 Spring 2013 #2

a. Define a *Euclidean domain.*

b. Define a *unique factorization domain.*

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

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

Solution omitted.

7.1.2 Fall 2017 #6

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

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

a. Prove R is an integral domain.

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

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

d. Show 3 is not prime in R.

e. Conclude R is not a PID.

Concept review omitted.

Solution omitted.

7.1.3 Spring 2017 #4

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

   Prove that R is not a UFD.

(You may assume Gauss' lemma)

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

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

Concept review omitted.

Solution omitted.

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

7.2.1 Fall 2021 #5

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

$$\operatorname{codim}_R I := \dim_{\mathbb{C}} R - \dim_{\mathbb{C}} I,$$

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

a. Show that any maximal ideal $m \subset R$ has codimension 1 .

b. Suppose that $\dim_C R = 2$. Show that there exists a surjective homomorphism of $\mathbb{C}$-algebras from the polynomial ring $\mathbb{C}[t]$ to R.

c. Classify such algebras R for which $\dim_{\mathbb{C}} R = 2$, and list their maximal ideals.

(DZG): my impression is that this is an unusually difficult problem, or was something specifically covered in this year's qual class.

7.2.2 Fall 2013 #3

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

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

Solution omitted.

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

Concept review omitted.

Solution omitted.

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.

Concept review omitted.

Solution omitted.

7.2.6 Spring 2018 #8

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

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

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

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

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

Solution omitted.

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 omitted.

7.3.2 Spring 2021 #5

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

Solution omitted.

7.3.3 Fall 2018 #7

Let R be a commutative ring.

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

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

is an R-module endomorphism of R.

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

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

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

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

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

Concept review omitted.

Solution omitted.

7.4 Zorn's Lemma

7.4.1 Fall 2013 #4

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

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

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

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

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

   Show that I is a prime ideal.

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

7.4.2 Fall 2015 #3

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

Prove that R contains a maximal left ideal.

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

Solution omitted.

7.4.3 Spring 2015 #7

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

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

Prove that every such ideal J is prime.

Solution omitted.

7.4.4 Spring 2013 #1

Let R be a commutative ring.

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

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

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

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

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

Prove that I is a prime ideal.

Solution omitted.

7.4.5 Fall 2019 #6

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

a. Show that

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

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.

Concept review omitted.

Solution omitted.

7.5 Noetherian Rings

7.5.1 Fall 2015 #4

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

Solution omitted.

7.5.2 Spring 2021 #6

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

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

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

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

c. Show that R is not Noetherian.

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

Solution omitted.

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.

Concept review omitted.

Solution omitted.

7.6.2 Spring 2016 #8

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

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

Prove the following:

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

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

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

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

Concept review omitted.

Solution omitted.

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 omitted.

Solution omitted.

7.7.2 Spring 2018 #5

Let

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

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

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

Solution omitted.

7.7.3 Spring 2014 #6

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

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

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

8 | Galois Theory

8.1 General Galois Extensions

8.1.1 Fall 2021 #4

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

a. What is the degree of $Q\left(\zeta_n\right)$ over Q ?

b. Define what it means for a finite field extension L/K to be Galois, and prove that the cyclotomic field $Q\left(\zeta_n\right)$ is Galois over $\mathbb{Q}$.

c. What is the Galois group of $\mathbb{Q}\left(\zeta_n\right)$ over $\mathbb{Q}$?

d. How many subfields of $\mathbb{Q}\left(\zeta_{2021}\right)$ 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 $G := \mathsf{Gal}(K/F)$ and $H := \mathsf{Gal}(K/E)$, and suppose H contains $N_G(P)$, where P is a Sylow p-subgroup of G for p a prime. Prove that $[E : F] \equiv 1 \bmod p$.

Concept review omitted.

Solution omitted.

8.1.3 Fall 2019 Midterm #9

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

Solution omitted.

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 omitted.

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

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

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

8.1.8 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 omitted.

8.1.9 Fall 2012 #4

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

8.2 Galois Groups: Concrete Computations

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

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

Solution omitted.

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 omitted.

8.2.3 Fall 2020 #3

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

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

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

Solution omitted.

8.2.4 Spring 2021 #4

Define

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

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

b. Find the Galois group G of f.

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

Concept review omitted.

Solution omitted.

8.2.5 Fall 2019 Midterm #6

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

8.2.6 Spring 2018 #2

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

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

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

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

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

Solution omitted.

8.2.7 Spring 2020 #4

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

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

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

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

8.2.8 Spring 2017 #8

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

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

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

8.2.9 Fall 2016 #4

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

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

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

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

8.2.10 Spring 2016 #2

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

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

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

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

8.2.11 Fall 2015 #5

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

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

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

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

8.2.12 Spring 2015 #5

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

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

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

8.2.13 Fall 2014 #3

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

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

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

8.2.14 Fall 2013 #6

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

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

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

Hint: what field is fixed by NH?

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

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

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

8.2.15 Spring 2014 #4

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

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

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

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

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

8.2.16 Spring 2013 #8

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

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

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

8.3 Galois Groups: Indirect Computations / Facts

8.3.1 Fall 2019 #7

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

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

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

Concept review omitted.

Solution omitted.

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.

Concept review omitted.

Solution omitted.

8.3.3 Spring 2018 #3

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

Let $E = E_1E_2 \subset K$.

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

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

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

c. Show that

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

Concept review omitted.

Solution omitted.

8.3.4 Fall 2017 #4

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

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

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

8.3.5 Spring 2017 #7

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

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

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

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

8.3.6 Spring 2016 #6

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

8.3.7 Fall 2015 #6

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

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 $|\text{Gal}(K/F)| = 12$. Prove that there exists an intermediate field E of K/F with $[E : F] = 3$.

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

8.3.8 Fall 2014 #1

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

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

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

8.3.9 Spring 2013 #7

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

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

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

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

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

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

8.3.10 Fall 2012 #3

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

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

8.4.1 Spring 2021 #7

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

Strategy omitted.

Solution omitted.

Strategy omitted.

Concept review omitted.

Solution omitted.

8.4.2 Fall 2019 #4

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

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

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

c. Prove that $m = k$.

Revisit, tricky!

Concept review omitted.

Solution omitted.

8.4.3 Spring 2019 #2

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

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

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

Concept review omitted.

Solution omitted.

8.4.4 ⋆ Fall 2016 #5

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

8.4.5 ⋆ Fall 2013 #7

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

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

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

8.5 General Field Extensions

8.5.1 Spring 2020 #3

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

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

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

8.5.2 Spring 2012 #1

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

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

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

8.5.3 Spring 2019 #8

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

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

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

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

Concept review omitted.

Solution omitted.

8.5.4 Fall 2017 #3

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

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

8.5.5 Spring 2015 #2

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

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

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

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

8.5.6 Spring 2014 #3

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

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

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

9 | Modules

9.1 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

$$\operatorname{Ann}(M) := \left\{r \in R \,\middle|\, r \cdot m = 0 \text{ for all } m \in M\right\}$$

a. Prove that $\operatorname{Ann}(M)$ 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 $\operatorname{Ann}(m) := \left\{r \in R \,\middle|\, r \cdot m = 0\right\}$, 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 $\operatorname{Tor}(M)$ is a submodule of M .

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

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

Concept review omitted.

Solution omitted.

9.2.2 ⋆ Spring 2019 #5

Let R be an integral domain. Recall that if M is an R-module, the *rank* of M is defined to be the maximum number of R-linearly independent elements of M .

a. Prove that for any R-module M, the rank of $\operatorname{Tor}(M)$ is 0.

b. Prove that the rank of M is equal to the rank of of $M/\operatorname{Tor}(M)$.

c. Suppose that M is a non-principal ideal of R.

Prove that M is torsion-free of rank 1 but not free.

Concept review omitted.

Solution omitted.

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 omitted.

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

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

Describe the elementary divisors and invariant factors of M.

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

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

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

a. Determine the elementary divisors and invariant factors of A.

b. Determine the minimal polynomial of A.

c. Determine the characteristic polynomial of A.

9.3 Misc/Unsorted

9.3.1 Spring 2017 #3

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

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

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

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

Solution omitted.

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

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

Concept review omitted.

Solution omitted.

9.3.4 Fall 2019 Final #2

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

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

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

9.3.5 Spring 2018 #6

Let

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

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

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

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

c. Use the previous part to describe M/N as a direct sum of cyclic $\mathbb{Z}$-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 $k \geq 0$.

9.3.7 Fall 2016 #6

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

9.3.8 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:

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

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

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

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

9.3.10 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 $\mathbb{Z}$-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

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

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

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

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

10 | Linear Algebra: Diagonalizability

10.1 Fall 2017 #7

Let F be a field and let V and W be vector spaces over F .

Make V and W into $F[x]$-modules via linear operators T on V and S on W by defining $X \cdot v = T(v)$ for all $v \in V$ and $X \cdot w = S(w)$ for all w ∈ W .

Denote the resulting $F[x]$-modules by V_T and W_S respectively.

a. Show that an $F[x]$-module homomorphism from V_T to W_S consists of an F-linear transformation $R : V \to W$ such that $RT = SR$.

b. Show that $VT \cong WS$ as $F[x]$-modules $\iff$ there is an F-linear isomorphism $P : V \to W$ such that $T = P^{-1}SP$.

c. Recall that a module M is *simple* if $M \neq 0$ and any proper submodule of M must be zero. Suppose that V has dimension 2. Give an example of F, T with V_T simple.

d. Assume F is algebraically closed. Prove that if V has dimension 2, then any V_T is not simple.

10.2 Spring 2015 #3

Let F be a field and V a finite dimensional F-vector space, and let $A, B : V \to V$ be commuting F-linear maps. Suppose there is a basis $\mathcal{B}_1$ with respect to which A is diagonalizable and a basis $\mathcal{B}_2$ with respect to which B is diagonalizable.

Prove that there is a basis $\mathcal{B}_3$ with respect to which A and B are both diagonalizable.

10.3 Fall 2016 #2

Let A, B be two $n \times n$ matrices with the property that $AB = BA$. Suppose that A and B are diagonalizable. Prove that A and B are *simultaneously* diagonalizable.

10.4 Spring 2019 #1

Let A be a square matrix over the complex numbers. Suppose that A is nonsingular and that A^{2019} is diagonalizable over $\mathbb{C}$.

Show that A is also diagonalizable over $\mathbb{C}$.

Concept review omitted.

Solution omitted.

11 Linear Algebra: Misc

11.1 ⋆ Spring 2012 #6

Let k be a field and let the group $G = \mathrm{GL}(m, k) \times \mathrm{GL}(n, k)$ acts on the set of $m \times n$ matrices $M_{m,n}(k)$ as follows:

$$(A, B) \cdot X = AXB^{-1}$$

where $(A, B) \in G$ and $X \in M_{m,n}(k)$.

a. State what it means for a group to act on a set. Prove that the above definition yields a group action.

b. Exhibit with justification a subset S of $M_{m,n}(k)$ which contains precisely one element of each orbit under this action.

11.2 ⋆ Spring 2014 #7

Let $G = \mathrm{GL}(3, \mathbb{Q}[x])$ be the group of invertible 3×3 matrices over $\mathbb{Q}[x]$. For each $f \in \mathbb{Q}[x]$, let S_f be the set of 3×3 matrices A over $\mathbb{Q}[x]$ such that $\det(A) = cf(x)$ for some nonzero constant $c \in \mathbb{Q}$.

a. Show that for $(P, Q) \in G \times G$ and $A \in S_f$, the formula

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

gives a well defined map $G \times G \times S_f \to S_f$ and show that this map gives a group action of $G \times G$ on S_f.

b. For $f(x) = x^3(x^2+1)^2$, give one representative from each orbit of the group action in (a), and justify your assertion.

11.3 Fall 2012 #7

Let k be a field of characteristic zero and $A, B \in M_n(k)$ be two square $n \times n$ matrices over k such that $AB - BA = A$. Prove that $\det A = 0$.

Moreover, when the characteristic of k is 2, find a counterexample to this statement.

11.4 Fall 2012 #8

Prove that any nondegenerate matrix $X \in M_n(\mathbb{R})$ can be written as $X = UT$ where U is orthogonal and T is upper triangular.

11.5 Fall 2012 #5

Let U be an infinite-dimensional vector space over a field k, $f : U \to U$ a linear map, and $\{u_1, \cdots, u_m\} \subset U$ vectors such that U is generated by $\left\{u_1, \cdots, u_m, f^d(u_1), \cdots, f^d(u_m)\right\}$ for some $d \in \mathbb{N}$.

Prove that U can be written as a direct sum $U \cong V \oplus W$ such that

1. V has a basis consisting of some vector $v_1, \cdots v_n, f^d(v_1), \cdots, f^d(v_n)$ for some $d \in \mathbb{N}$, and
2. W is finite-dimensional.

Moreover, prove that for any other decomposition $U \cong V' \oplus W'$, one has $W' \cong W$.

11.6 Fall 2015 #7

a. Show that two 3×3 matrices over $\mathbb{C}$ are similar $\iff$ their characteristic polynomials are equal and their minimal polynomials are equal.

b. Does the conclusion in (a) hold for 4×4 matrices? Justify your answer with a proof or counterexample.

11.7 Fall 2014 #4

Let F be a field and T an $n \times n$ matrix with entries in F. Let I be the ideal consisting of all polynomials $f \in F[x]$ such that $f(T) = 0$.

Show that the following statements are equivalent about a polynomial $g \in I$:

a. g is irreducible.

b. If $k \in F[x]$ is nonzero and of degree strictly less than g, then $k[T]$ is an invertible matrix.

11.8 Fall 2015 #8

Let V be a vector space over a field F and $V^\vee$ its dual. A *symmetric bilinear form* $(-,-)$ on V is a map $V \times V \to F$ satisfying

$$(av_1 + bv_2, w) = a(v_1, w) + b(v_2, w) \quad \text{and} \quad (v_1, v_2) = (v_2, v_1)$$

for all $a, b \in F$ and $v_1, v_2 \in V$. The form is *nondegenerate* if the only element $w \in V$ satisfying $(v, w) = 0$ for all $v \in V$ is $w = 0$.

Suppose $(-,-)$ is a nondegenerate symmetric bilinear form on V. If W is a subspace of V, define

$$W^\perp := \left\{ v \in V \;\middle|\; (v, w) = 0 \text{ for all } w \in W \right\}.$$

a. Show that if X, Y are subspaces of V with $Y \subset X$, then $X^\perp \subseteq Y^\perp$.

b. Define an injective linear map

$$\psi : Y^\perp / X^\perp \hookrightarrow (X/Y)^\vee$$

which is an isomorphism if V is finite dimensional.

11.9 Fall 2018 #4

Let V be a finite dimensional vector space over a field (the field is not necessarily algebraically closed).

Let $\varphi : V \to V$ be a linear transformation. Prove that there exists a decomposition of V as $V = U \oplus W$, where U and W are φ-invariant subspaces of V , $\varphi|_U$ is nilpotent, and $\varphi|_W$ is nonsingular.

Revisit.

Solution omitted.

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.

Concept review omitted.

Strategy omitted.

Solution omitted.

11.11 Fall 2019 #8

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

$$\Lambda := \left\{ \sum r_i e_i \,\middle|\, r_i \in \mathbb{Z} \right\}$$

Let $\cdot$ be a non-degenerate ($v \cdot w = 0$ for all $w \in V \iff v = 0$) symmetric bilinear form on V such that the Gram matrix $M = (e_i \cdot e_j)$ has integer entries.

Define the dual of Λ to be

$$\Lambda^\vee := \left\{ v \in V \,\middle|\, v \cdot x \in \mathbb{Z} \text{ for all } x \in \Lambda \right\}.$$

a. Show that $\Lambda \subset \Lambda^\vee$.

b. Prove that $\det M \neq 0$ and that the rows of M^{-1} span $\Lambda^\vee$.

c. Prove that $\det M = |\Lambda^\vee / \Lambda|$.

Todo, missing part (c).

Solution omitted.

Solution omitted.

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?

Concept review omitted.

Solution omitted.

11.13 Fall 2020 #8

Let $A \in \operatorname{Mat}(n \times n, \mathbb{C})$ such that the group generated by A under multiplication is finite. Show that

$$\operatorname{Tr}(A^{-1}) = \overline{\operatorname{Tr}(A)},$$

where $\overline{(-)}$ denotes taking the complex conjugate and $\operatorname{Tr}(-)$ is the trace.

12 | Linear Algebra: Canonical Forms

12.1 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. $\mathrm{rk}A = 5$,

c. $\mathrm{rk}A^2 = 4$,

d. $\mathrm{rk}A - I = 6$,

e. $\mathrm{rk}A^3 - I = 4$,

f. $\operatorname{tr} A = 1$?

Solution omitted.

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 $\mathbb{C}$. Prove the Cayley-Hamilton theorem: if $p(x)$ is the characteristic polynomial of T, then $p(T) = 0$. You may use canonical forms.

12.4 ⋆ Spring 2012 #7

Consider the following matrix as a linear transformation from $V := \mathbb{C}^5$ to itself:

$$A = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 \\ -4 & 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

a. Find the invariant factors of A.

b. Express V in terms of a direct sum of indecomposable $\mathbb{C}[x]$-modules.

c. Find the Jordan canonical form of A.

12.5 Fall 2019 Final #8

Exhibit the rational canonical form for

- $A \in M_6(\mathbb{Q})$ with minimal polynomial $(x-1)(x^2+1)^2$.
- $A \in M_{10}(\mathbb{Q})$ with minimal polynomial $(x^2+1)^2(x^3+1)$.

12.6 Fall 2019 Final #9

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

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

12.7 Spring 2016 #7

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

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

Determine the elementary divisors and invariant factors of M.

12.8 Spring 2020 #7

Let

$$A = \begin{bmatrix} 2 & 0 & 0 \\ 4 & 6 & 1 \\ -16 & -16 & -2 \end{bmatrix} \in M_3(\mathrm{C}).$$

a. Find the Jordan canonical form J of A.

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

c. Write down the minimal polynomial of A.

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

12.9 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 $F = \mathbb{Q}$,

b. When $F = \mathbb{F}_p$.

Hint: In both cases, all eigenvalues lie in the ground field. In each case find a matrix P such that $P^{-1}AP$ is in JCF.

Strategy omitted.

Concept review omitted.

Solution omitted.

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 $M_n(\mathbb{C})$?

b. Find a nonzero matrix $P \in M_n(\mathbb{C})$ such that $P^{-1}AP$ is in Jordan canonical form.

12.12 Spring 2016 #1

Let

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

a. Find the Jordan canonical form J of A.

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

12.13 Spring 2015 #6

Let F be a field and n a positive integer, and consider

$$A = \begin{bmatrix} 1 & \dots & 1 \\ & \ddots & \\ 1 & \dots & 1 \end{bmatrix} \in M_n(F).$$

Show that A has a Jordan normal form over F and find it.

Hint: treat the cases $n \cdot 1 \neq 0$ in F and $n \cdot 1 = 0$ in F separately.

12.14 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 $\mathbb{C}$-vector space to itself and suppose $f(T) = 0$ where $f(x) = x^2 + 2x + 1$.

a. Show that there does not exist any vector $v \in V$ such that $Tv = v$, but there *does* exist a vector $w \in V$ such that $T^2 w = w$.

b. Give all of the possible Jordan canonical forms of T.

12.16 Spring 2021 #1

Let m

$$A := \begin{bmatrix} 4 & 1 & -1 \\ -6 & -1 & 2 \\ 2 & 1 & 1 \end{bmatrix} \in \mathrm{Mat}(3 \times 3, \mathbb{C}).$$

a. Find the Jordan canonical form J of A.

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

c. Write down the minimal polynomial of A.

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

Concept review omitted.

Solution omitted.

12.17 Fall 2020 #5

Consider the following matrix:

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

a. Find the minimal polynomial of B.

b. Find a 3×3 matrix J in Jordan canonical form such that $B = JPJ^{-1}$ where P is an invertible matrix.

13 Extra Problems

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
$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow \cdots V_k \longrightarrow 0$$
is exact. Prove that $\sum_{i=1}^{k} (-1)^i \dim_D V_i = 0$.
2. Prove that if A and B are invertible matrices over a field $\boldsymbol{k}$, then $A + \lambda B$ is invertible for all but finitely many $\lambda \in \boldsymbol{k}$.
3. For the ring of $n \times n$ matrices over a commutative unital ring R, which we'll denote $\operatorname{Mat}_n(R)$, 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 $\boldsymbol{k}$, so $\varphi\psi = \psi\varphi$.

- Prove that if k is algebraically closed, then φ and ψ have a common eigenvector.
- Prove that if E has a basis consisting of eigenvectors of φ and E has a basis consisting of eigenvectors of ψ, then E has a basis consisting of vectors that are eigenvectors for both φ and ψ simultaneously.

13.2 Galois Theory

Taken from here: https://math.ucr.edu/~mpierce/teaching/qual-algebra/fun/galois/

1. Suppose that for an extension field F over K and for $a \in F$, we have that $b \in F$ is algebraic over $K(a)$ but transcendental over K. Prove that a is algebraic over $K(b)$.
2. Suppose that for a field F/K that $a \in F$ is algebraic and has odd degree over K. Prove that a^2 is also algebraic and has odd degree over K, and furthermore that $K(a) = K\left(a^2\right)$
3. For a polynomial $f \in K[x]$, prove that if $r \in F$ is a root of f then for any $\sigma \in \mathbf{Aut}_K F, \sigma(r)$ is also a root of f
4. Prove that as extensions of $\boldsymbol{Q}, \boldsymbol{Q}(x)$ is Galois over $\boldsymbol{Q}\left(x^2\right)$ but not over $\boldsymbol{Q}\left(x^3\right)$.
5. If F is over E, and E is over K is F necessarily over K ? Answer this question for each of the words "algebraic," "normal," and "separable" in the blanks.
6. If F is over K, and E is an intermediate extension of F over K, is F necessarily over E? Answer this question for each of the words "algebraic," "normal," and "separable" in the blanks.
7. If F is some (not necessarily Galois) field extension over K such that $[F : K] = 6$ and Aut ${}_K F \simeq S_3$, then F is the splitting field of an irreducible cubic over $K[x]$.
8. Recall the definition of the join of two subgroups $H \vee G$ (or $H+G$). For F a finite dimensional Galois extension over K and let A and B be intermediate extensions. Prove that

a. $\mathrm{Aut}_{AB}\, F = \mathrm{Aut}_A F \cap \mathrm{Aut}_B F$
b. Aut ${}_{A\cap B} F = \mathrm{Aut}_A F \vee \mathrm{Aut}_B F$

9. For a field K take $f \in K[x]$ and let $n = \deg f$. Prove that for a splitting field F of f over K that $[F : K] \leq n!$. Furthermore prove that $[F : K]$ divides $n!$.
10. Let F be the splitting field of $f \in K[x]$ over K. Prove that if $g \in K[x]$ is irreducible and has a root in F, then g splits into linear factors over F.
11. Prove that a finite field cannot be algebraically closed.
12. For $u = \sqrt{2+\sqrt{2}}$, What is the Galois group of $\boldsymbol{Q}(u)$ over $\boldsymbol{Q}$? What are the intermediate fields of the extension $\boldsymbol{Q}(u)$ over $\boldsymbol{Q}$?
13. Characterize the splitting field and all intermediate fields of the polynomial $\left(x^2-2\right)\left(x^2-3\right)\left(x^2-5\right)$ over Q. Using this characterization, find a primitive element of the splitting field.
14. Characterize the splitting field and all intermediate fields of the polynomial $x^4 - 3$ over Q
15. Consider the polynomial $f = x^3 - x + 1$ in $\boldsymbol{F}_3[x]$. Prove that f is irreducible. Calculate the degree of the splitting field of f over $\boldsymbol{F}_3$ and the cardinality of the splitting field of f.
16. Given an example of a finite extension of fields that has infinitely many intermediate fields.
17. Let $u = \sqrt{3+\sqrt{2}}$. Is $\boldsymbol{Q}(u)$ a splitting field of u over $\boldsymbol{Q}$? (MathSE)
18. Prove that the multiplicative group of units of a finite field must be cyclic, and so is generated by a single element.
19. Prove that $\boldsymbol{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\boldsymbol{F}_p$.
20. Prove that for any positive integer n there is an irreducible polynomial of degree n over $\boldsymbol{F}_p$

21. Recall the definition of a perfect field. Give an example of an imperfect field, and the prove that every finite field is perfect.
22. For $n > 2$ let ζ_n denote a primitive n th root of unity over Q. Prove that
$$\left[\boldsymbol{Q}\left(\zeta_n + \zeta_n^{-1} : \boldsymbol{Q}\right)\right] = \frac{1}{2}\varphi(n)$$
where φ is Euler's totient function.
23. Suppose that a field K with characteristic not equal to 2 contains an primitive n th root of unity for some odd integer n. Prove that K must also contain a primitive $2n$ th root of unity.
24. Prove that the Galois group of the polynomial $x^n - 1$ over Q is abelian.

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 $\langle 2, x\rangle \trianglelefteq \mathbb{Z}[x]$ is not a principal ideal.
- Let R be a Noetherian ring and A, B algebras over R. Suppose A is finite type over R and finite over B. Then B is finite type over R.

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 H equals the index of the normalizer of H.
- Show that $Z(G) = \bigcap_{a\in G} C_G(a)$.
- Show that the centralizer $G_G(H)$ of a subgroup is again a subgroup.
- Show that $C_G(H) \trianglelefteq N_G(H)$ is a normal subgroup.

- Show that $C_G(G) = Z(G)$.

- Show that for $H \leq G$, $C_H(x) = H \cap C_G(x)$.

- Let $H, K \leq G$ a finite group, and without using the normalizers of H or K, show that $|HK| = |H||K|/|H \cap K|$.

- Show that if $H \leq N_G(K)$ then $HK \leq H$, and give a counterexample showing that this condition is necessary.

- Show that HK is a subgroup of G iff $HK = KH$.

- Prove that the kernel of a homomorphism is a normal subgroup.

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:

◊ $|h| = p^3$
◊ $|h| = p$.

Hint: Sylow and semidirect products.

- Show that any normal p- subgroup is contained in every Sylow p-subgroup of G.
- Show that the order of $1+p$ in $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^{\times}$ is equal to p. Use this to construct a non-abelian group of order p^3.

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 $O_p(G) \trianglelefteq G$, is maximal among all normal p-subgroups of G
- Let $P \in \mathrm{Syl}_p(H)$ where $H \trianglelefteq G$ and show that $P \cap H \in \mathrm{Syl}_p(H)$.
- Show that Sylow p_i-subgroups S_{p_1}, S_{p_2} for distinct primes $p_1 \neq p_2$ intersect trivially.
- Show that in a p group, every normal subgroup intersects the center nontrivially.

13.4.4 Symmetric Groups

Specific Groups

- Show that the center of S_3 is trivial.

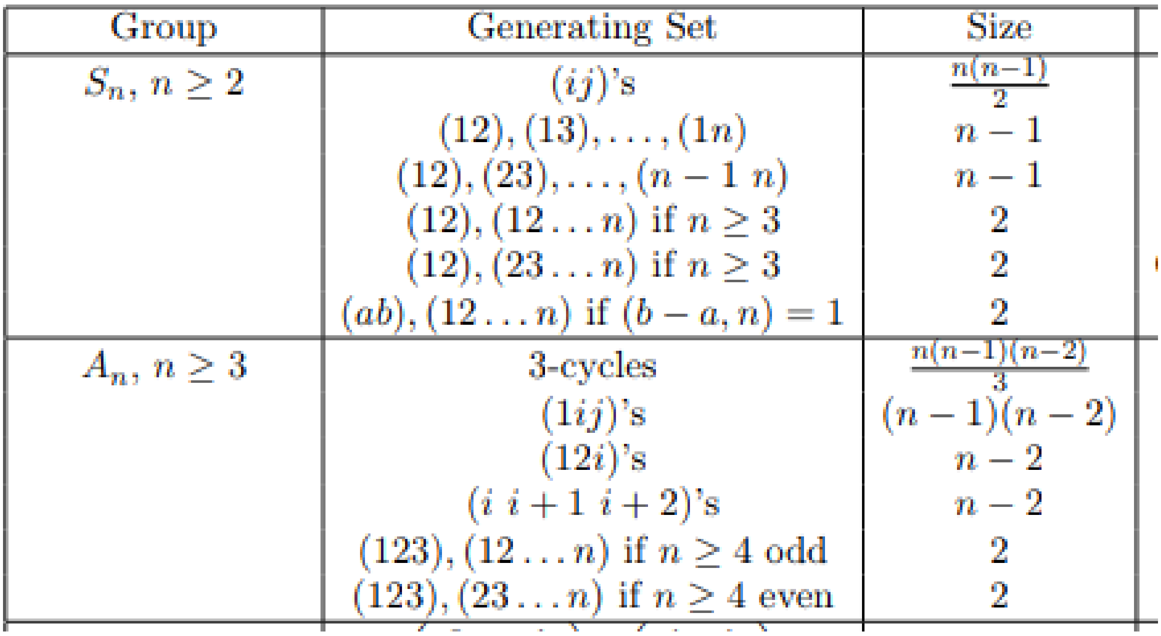
- Show that $Z(S_n) = 1$ for $n \geq 3$
- Show that $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \cong S_3$.
- Show that the transitive subgroups of S_3 are S_3, A_3
- Show that the transitive subgroups of S_4 are $S_4, A_4, D_4, \mathbb{Z}_2^2, \mathbb{Z}_4$.
- Show that S_4 has two normal subgroups: $A_4, \mathbb{Z}_2^2$.
- Show that $S_{n\geq 5}$ has one normal subgroup: A_n.
- $Z(A_n) = 1$ for $n \geq 4$
- Show that $[S_n, S_n] = A_n$
- Show that $[A_4, A_4] \cong \mathbb{Z}_2^2$
- Show that $[A_n, A_n] = A_n$ for $n \geq 5$, so $A_{n\geq 5}$ is nonabelian.

General Structure

- Show that an m-cycle is an odd permutation iff m is an even number.
- Show that a permutation is odd iff it has an odd number of even cycles.
- Show that the center of S_n for $n \geq 4$ is nontrivial.
- Show that disjoint cycles commute.
- Show directly that any k-cycle is a product of transpositions, and determine how many transpositions are needed.

Generating Sets

- Show that S_n is generated by any of the following types of cycles:



Group	Generating Set	Size
S_n, $n \geq 2$	(ij)'s	$\frac{n(n-1)}{2}$
	$(12), (13), \ldots, (1n)$	$n-1$
	$(12), (23), \ldots, (n-1\ n)$	$n-1$
	$(12), (12\ldots n)$ if $n \geq 3$	2
	$(12), (23\ldots n)$ if $n \geq 3$	2
	$(ab), (12\ldots n)$ if $(b-a, n) = 1$	2
A_n, $n \geq 3$	3-cycles	$\frac{n(n-1)(n-2)}{3}$
	$(1ij)$'s	$(n-1)(n-2)$
	$(12i)$'s	$n-2$
	$(i\ i+1\ i+2)$'s	$n-2$
	$(123), (12\ldots n)$ if $n \geq 4$ odd	2
	$(123), (23\ldots n)$ if $n \geq 4$ even	2

  - Show that S_n is generated by transpositions.
  - Show that S_n is generated by *adjacent* transpositions.
  - Show that S_n is generated by $\{(12), (12\cdots n)\}$ for $n \geq 2$

  - Show that S_n is generated by $\{(12), (23 \cdots n)\}$ for $n \geq 3$
  - Show that S_n is generated by $\{(ab), (12 \cdots n)\}$ where $1 \leq a < b \leq n$ iff $\gcd(b-a, n) = 1$.
  - Show that S_p is generated by any arbitrary transposition and any arbitrary p-cycle.

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 $n \geq 5$.
- Show that $\mathrm{Out}(A_4)$ is nontrivial.

13.4.6 Dihedral Groups

- Show that if $N \trianglelefteq D_n$ is a normal subgroup of a dihedral group, then D_n/N is again a dihedral group.

13.4.7 Other Groups

- Show that $\mathbb{Q}$ is not finitely generated as a group.
- Show that the Quaternion group has only one element of order 2, namely -1.

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 $n \geq 5$
- Give a necessary and sufficient condition for a cyclic group to be solvable.
- Prove that every simple abelian group is cyclic.
- Show that S_n is generated by disjoint cycles.
- Show that S_n is generated by transpositions.
- Show if G is finite, then G is solvable $\iff$ all of its composition factors are of prime order.
- Show that if N and G/N are solvable, then G is solvable.
- Show that if G is finite and solvable then every composition factor has prime order.
- Show that G is solvable iff its derived series terminates.
- Show that S_3 is not nilpotent.
- Show that G nilpotent $\implies$ G solvable
- Show that nilpotent groups have nontrivial centers.
- Show that Abelian $\implies$ nilpotent
- Show that p-groups $\implies$ nilpotent

13.4.11 Misc

- Prove Burnside's theorem.
- Show that $\text{Inn}(G) \trianglelefteq Aut(G)$
- Show that $\text{Inn}(G) \cong G/Z(G)$

- Show that the kernel of the map $G \to \mathrm{Aut}(G)$ 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 $H \leq G$, $K \trianglelefteq G$ is a normal subgroup, and H char K then H is normal in G.

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

13.5 Ring Theory

13.5.1 Basic Structure

- Show that if an ideal $I \trianglelefteq R$ contains a unit then $I = R$.
- Show that $R^\times$ need not be closed under addition.

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 omitted.

Problem 13.5.2 (Maximal implies prime)
Maximal $\implies$ prime, but generally not the converse.

Solution omitted.

- Show that every proper ideal is contained in a maximal ideal
- Show that if $x \in R$ a PID, then x is irreducible $\iff \langle x \rangle \trianglelefteq R$ is maximal.
- Show that intersections, products, and sums of ideals are ideals.
- Show that the union of two ideals need not be an ideal.
- Show that every ring has a proper maximal ideal.
- Show that $I \trianglelefteq R$ is maximal iff R/I is a field.
- Show that $I \trianglelefteq R$ is prime iff R/I is an integral domain.
- Show that $\cup_{\mathfrak{m} \in \operatorname{maxSpec}(R)} = R \setminus R^\times$.
- Show that $\operatorname{maxSpec}(R) \subsetneq \operatorname{Spec}(R)$ but the containment is strict.
- Show that every prime ideal is radical.
- Show that the nilradical is given by $\sqrt{0_R} = \sqrt{(0)}$.
- Show that $\operatorname{rad}(IJ) = \operatorname{rad}(I) \cap \operatorname{rad}(J)$
- Show that if $\operatorname{Spec}(R) \subseteq \operatorname{maxSpec}(R)$ then R is a UFD.
- Show that if R is Noetherian then every ideal is finitely generated.

13.5.3 Characterizing Certain Ideals

- Show that for an ideal $I \trianglelefteq R$, its radical is the intersection of all prime ideals containing I.
- Show that $\sqrt{I}$ is the intersection of all prime ideals containing I.

Problem 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 omitted.

Problem 13.5.4 (Mod by nilradical to kill nilpotents)
$R/\sqrt{0_R}$ has no nonzero nilpotent elements.

Solution omitted.

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 omitted.

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

Extensions?

- What is $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}]$?
- What is $[\mathbb{Q}(2^{\frac{3}{2}}) : \mathbb{Q}]$?
- Show that if $p \in \mathbb{Q}[x]$ and $r \in \mathbb{Q}$ is a rational root, then in fact $r \in \mathbb{Z}$.
- If $\{\alpha_i\}_{i=1}^n \subset F$ are algebraic over K, show that $K[\alpha_1, \cdots, \alpha_n] = K(\alpha_1, \cdots, \alpha_n)$.
- Show that α/F is algebraic $\iff$ $F(\alpha)/F$ is a finite extension.
- Show that every finite field extension is algebraic.
- Show that if α, β are algebraic over F, then $\alpha \pm \beta, \alpha\beta^{\pm 1}$ are all algebraic over F.
- Show that if $L/K/F$ with K/F algebraic and L/K algebraic then L is algebraic.

Special Polynomials

- Show that a field with p^n elements has exactly one subfield of size p^d for every d dividing n.

- Show that $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n.
- Show that $x^{p^d} - x \mid x^{p^n} - x \iff d \mid n$
- Prove that $x^{p^n} - x$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ with degree dividing n.
- Prove that an irreducible $\pi(x) \in \mathbb{F}_p[x]$ divides $x^{p^n} - x \iff \deg \pi(x)$ divides n.

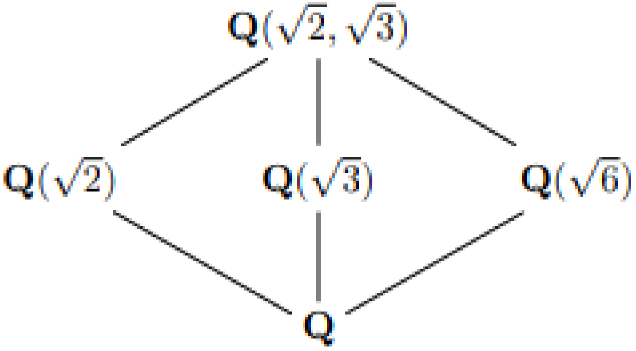
13.7 Galois Theory

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 $\operatorname{ch}(F) \neq 2$ 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 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, show it is equal to $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, and find a corresponding minimal polynomial.



- Compute all intermediate field extensions of $\mathbb{Q}(2^{\frac{1}{4}}, \zeta_8)$.
- Show that $\mathbb{Q}(2^{\frac{1}{3}})$ and $\mathbb{Q}(\zeta_3 2^{\frac{1}{3}})$

- Show that if L/K is separable, then L is normal $\iff$ there exists a polynomial $p(x) = \prod_{i=1}^{n} x - \alpha_i \in K[x]$ such that $L = K(\alpha_1, \cdots, \alpha_n)$ (so L is the splitting field of p).
- Is $\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}$ normal?
- Show that $\mathbb{GF}(p^n)$ is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.
- Show that $\mathbb{GF}(p^d) \leq \mathbb{GF}(p^n) \iff d \mid n$
- Compute the Galois group of $x^n - 1 \in \mathbb{Q}[x]$ as a function of n.
- Identify all of the elements of the Galois group of $x^p - 2$ for p an odd prime (note: this has a complicated presentation).
- Show that $\text{Gal}(x^{15} + 2)/\mathbb{Q} \cong S_2 \rtimes \mathbb{Z}/15\mathbb{Z}$ for S_2 a Sylow 2-subgroup.
- Show that $\text{Gal}(x^3 + 4x + 2)/\mathbb{Q} \cong S_3$, 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 $A \in \text{Mat}(n \times n, \mathbb{Z})$ is finite $\iff$ $\det A \neq 0$, and show that in this case $|\text{coker}(A)| = |\det(A)|$.
- Show that a nilpotent operator is diagonalizable.
- Show that if A, B are diagonalizable and $[A, B] = 0$ then A, B are simultaneously diagonalizable.
- Does diagonalizable imply invertible? The converse?
- Does diagonalizable imply distinct eigenvalues?
- Show that if a matrix is diagonalizable, its minimal polynomial is squarefree.
- Show that a matrix representing a linear map $T : V \to V$ is diagonalizable iff V is a direct sum of eigenspaces $V = \bigoplus_i \ker(T - \lambda_i I)$.
- Show that if $\{\mathbf{v}_i\}$ is a basis for V where $\dim(V) = n$ and $T(\mathbf{v}_i) = \mathbf{v}_{i+1 \bmod n}$ then T is diagonalizable with minimal polynomial $x^n - 1$.
- Show that if the minimal polynomial of a linear map T is irreducible, then every T-invariant subspace has a T-invariant complement.

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 $\mathrm{SL}_2(Z)$?

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 $n \geq 5$.

14.1.22 Question 1.22

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

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 $\mathrm{SL}_2(R)$ acting on $\mathbb{R}^2$ by matrix multiplication. What is the stabiliser of a point? Does it depend which point? Do you know what sort of subgroup this is? What if $\mathrm{SL}_2(R)$ acts by Möbius transformations instead?

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 $\mathbb{Q}$. How many are there? Are the ones you've given involving denominators divisible only by certain primes distinct? So that gives you the cardinality. Are these all of them?

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 $\mathbb{F}_p$, for p prime. What does basic group theory tell us about G?

How many conjugates does a Sylow p-subgroup have? Give a matrix form for the elements in this subgroup.

Explain the conjugacy in terms of eigenvalues and eigenvectors. give a matrix form for the normaliser of the Sylow p-subgroup.

14.1.39 Question 1.39

Let's look at $\mathrm{SL}_2(\mathbb{F}_3)$. How many elements are in that group? What is its centre? Identify $\mathrm{PSL}_2(\mathbb{F}_3)$ as a permutation group.

14.1.40 Question 1.40

How many elements does $\mathfrak{gl}_2(\mathbb{F}_q)$ have? How would you construct representations?

What can you say about the 1-dimensional representations? What can you say about simplicity of some related groups?

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 $\mathbb{Z}^2$?

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 $\mathbb{Q}$?

14.2.3 Question 2.3

State/prove the Sylow theorems.

14.2.4 Question 2.4

Classify groups of order 35.

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 $1 \bmod p$?

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 $\mathbb{F}_p^n$ over $\mathbb{F}_p$. 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 $\mathbb{F}_9$?

14.3.7 Question 3.7

What is a separable extension? Can $\mathbb{Q}$ have a non-separable extension? How about $\mathbb{Z}/p\mathbb{Z}$? Why not? Are all extensions of characteristic 0 fields separable? Of finite fields? Prove it.

Give an example of a field extension that's not separable.

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 $\mathbb{Q}$? What are the intermediate extensions? Which extensions are normal, which are not, and why? What are the Galois groups (over Q) of all intermediate extensions?

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 $\mathsf{Gal}(K/F)$ 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 $\mathbb{Q}(\sqrt[3]{21})$ 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 $\mathbb{Z}$ in $\mathbb{Q}(i)$?

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

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

14.3.24 Question 3.24

What is the Galois group of

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

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 $\mathbb{Q}$. 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 $\mathbb{Q}$ 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 $\mathbb{Q}$?

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 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$?

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 $\mathbb{Q}$?

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 $\mathbb{Q}$ 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 $K/\mathbb{Q}$ by $f(x) \in \mathbb{Z}[x]$ such that $\deg(f) = n$ and $\mathsf{Gal}(K/Q) = S_n$. What can you say about the roots?

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 $\mathbb{C}$? How can you extend a subfield automorphism? What feature of $\mathbb{C}$ 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 mth root of unity. Prove that if p divides $f(a)$ for some integer a and $\gcd(p, m) = 1$ then m divides $p - 1$. Use this fact to show that there are infinitely many primes congruent to $1 \bmod m$.

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 $\mathbb{F}_2$?

14.3.60 Question 3.60

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

14.3.61 Question 3.61

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

14.3.62 Question 3.62

For each prime p, give a polynomial of degree p that is irreducible over $\mathbb{F}_p$. You can do it in a "uniform" way.

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 $\mathbb{Q}$?

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 $\mathrm{Mat}(n \times n, \mathbb{C})$, are they necessarily conjugate in $\mathrm{Mat}(n \times N, R)$ 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 $SL_n(\mathbb{R})$. Does A also have to be in $\mathrm{SL}_n(R)$? 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 $\mathrm{SL}_2(\mathbb{R})$?

14.4.21 Question 4.21

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

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 $\mathbb{R}^2$?

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 $\mathbb{Z}/p\mathbb{Z}$?

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 $\mathbb{C}[x, y]$ 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 $\mathbb{Q}[x]$ say about factorisation over $\mathbb{Z}[x]$?

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 $\mathbb{Z}$ in $\mathbb{Q}(i)$?

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 $\mathbb{Z}$" mean?

14.6.18 Question 6.18

Let $\mathcal{O}$ be the ring of integers of $\mathbb{Q}(d)$, where $d > 0$. What can you say about the quotient of O by one of its prime ideals?

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 $R[x_1, \cdots, x_n]$ is a unique factorisation domain? What is wrong with unique factorisation if we don't have a domain? Now, PIDs are Noetherian, but are there UFDs which are not?

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 $\mathbb{Z}$?

14.6.25 Question 6.25

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

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 $\mathbb{Z}[x]$?

14.6.29 Question 6.29

Is the following map an isomorphism?

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

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 $\operatorname{Mat}(n \times n, K)$ with $\underset{K}{\operatorname{End}}(V)$ where V is an n-dimensional K-vector space. Try to geometrically describe the simple left ideals and also the simple right ideals via that identification.

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 $\mathbb{C}$ endowed with the usual law of addition and the following analogue of the convolution product:

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

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

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 $\mathbb{R}$.

14.6.50 Question 6.50

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

14.6.51 Question 6.51

What is Wedderburn's theorem? What does the group ring generated by $\mathbb{Z}/5\mathbb{Z}$ over $\mathbb{Q}$ look like?

What if we take the noncyclic group of order 4 instead of $\mathbb{Z}/5\mathbb{Z}$? The quaternion group instead of $\mathbb{Z}/5\mathbb{Z}$?

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 $\mathbb{Z}$)? 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 $\mathbb{Z}$, 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, $\mathbb{Z}$-modules. Take $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$, where p and q are distinct primes. What is their tensor product?

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 $\mathbb{C}$ in the definition of group algebra?

Is it possible to work over other fields?

What goes wrong if the characteristic of the field divides the order of the group?

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 $\mathrm{GL}(V)$ 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 $\mathbb{Z}$, the infinite cyclic group. What is the group algebra of $\mathbb{Z}$?

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 $\mathbb{Z}$ 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 finite-dimensional 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 $\mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$? What is $\mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})$?