

# ALGEBRA EXAM BREAKDOWN

September 24, 2019

## CONTENTS

1. Overview	3
2. Spring 2019	4
3. Fall 2018	5
4. Spring 2018	6
5. Fall 2017	7
6. Spring 2017	8
7. Fall 2016	9
8. Spring 2016	10
9. Fall 2015	12
10. Spring 2015	14
11. Fall 2014	16
12. Spring 2014	18
13. Fall 2013	19
14. Spring 2013	21
15. Fall 2011	22
16. Spring 2011	23
17. Fall 2010	24
18. Spring 2010	25
19. Fall 2009	27
20. Spring 2008	29
21. Fall 2007	30
22. Fall 2006	32
23. Spring 2006	33
24. Spring 2005	34

25. Fall 2004	35
26. Spring 2004	37
27. Fall 2002	38
28. Fall 2000	39
29. Fall 1997	40
30. Fall 1996	42
Concept Index	43

## 1. OVERVIEW

This is a collection of past comprehensive exams in analysis offered at Western.

### 1.1. Caveat emptor.

- The list of exams is *not* comprehensive:  
There are several gaps among old exams, and we do not intend to fill them.
- This document is likely to have mistakes:  
A team of us<sup>1</sup> typeset scans of the original exams, and we may have introduced typos.
- Not every problem was reproduced exactly from the original:  
We made occasional minor editorial changes, some of which are highlighted in [blue](#).
- There are *no* solutions:  
The best way to study is to write your own solutions.
- The exams are in the order in which the reader is intended to work through them:  
Upcoming exams are more likely to resemble recent exams than old exams.

### 1.2. Features.

- In most problem statements, many key terms are highlighted in [magenta](#).
- An index of common concepts appears at the end.

If you have comments or would like to contribute to the document, please contact Chris Hall ([cha1169@uwo.ca](mailto:cha1169@uwo.ca)).

---

<sup>1</sup>Félix Baril Boudreau, Sergio Zapata Ceballos, Chris Hall, Andrew Herring, Udit Mavinkurve, Mohabat Tarkeshian

2. SPRING 2019

1. Let  $G$  be a **simple group** and denote its **order** by  $|G|$ . Suppose that  $1 < |G| \leq 30$ . Show that  $|G| = p$  a prime number.

2. Consider the  **$\mathbb{Z}$ -module homomorphism**

$$f: \mathbb{Z}^3 \rightarrow \mathbb{Z}^3$$

given by the matrix

$$\begin{bmatrix} -7 & -8 & -8 \\ 4 & 4 & 4 \\ 12 & 0 & 12 \end{bmatrix}.$$

Find  $|\text{coker}(f)|$  where  $\text{coker}(f)$  is the **cokernel**.

3. Let  $F$  be a **field** with 5 elements. Let  $S$  be the collection of **similarity classes** of matrices over  $F$  with **minimal polynomial**  $(x-1)(x^2+x+1)^2$  and **characteristic polynomial**  $(x-1)^2(x^2+x+1)^4$ . What is  $|S|$ ?

4. Assume that  $K/F$  is a **finite Galois extension**,  $G = \text{Gal}(K/F)$  is its **Galois group**, and  $\alpha$  is in  $K^\times := K \setminus \{0\}$ . Also assume  $\text{char}(F) \neq 2$ . (This means that  $1+1 \neq 0$  in  $F$ .)

Show that  $K(\sqrt{\alpha})/F$  is also a Galois extension if and only if  $\frac{\sigma(\alpha)}{\alpha} \in K^{\times 2}$  for every  $\sigma \in G$  where  $K^{\times 2} = \{\beta^2 : \beta \in K^\times\}$ .

5. Consider  $K = \mathbb{Q}(\sqrt{5})$  and  $L = \mathbb{Q}(\sqrt{7})$ . Decide which of these fields can be embedded into a **Galois extension**  $N/\mathbb{Q}$  such that  $\text{Gal}(N/\mathbb{Q})$  is a **cyclic group** of order 4.

6. Let  $\text{GL}_3(\mathbb{F}_p)$  be the **group of invertible matrices**  $3 \times 3$  over  $\mathbb{F}_p$ . ( $\mathbb{F}_p$  is the **finite field** with  $p$  elements,  $p$  is a prime number.) Consider the set of matrices  $U_3(\mathbb{F}_p)$  which are **upper triangular** and have all elements on diagonal 1. (Below the diagonal, all elements are zero. On the diagonal, all elements are 1, and above the diagonal, any entries from  $\mathbb{F}_p$  are possible.)

Show that  $U_3(\mathbb{F}_p)$  is a  **$p$ -Sylow subgroup** of  $\text{GL}_3(\mathbb{F}_p)$ .

7. Consider the following in  $\mathbb{Z}[\sqrt{7}] = \{a + b\sqrt{7} : a, b \in \mathbb{Z}\}$ .

(a) Show that 9 **factors** as  $3 \cdot 3$  but is also equal to  $(4 + \sqrt{7})(4 - \sqrt{7})$  (this is easy).

(b) Each of the elements  $3, 4 + \sqrt{7}, 4 - \sqrt{7}$  are **irreducible**, i.e., if  $4 + \sqrt{7} = w \cdot W$  with  $w, W \in \mathbb{Z}[\sqrt{7}]$ , then  $w \mid 1$  or  $W \mid 1$  (where  $a \mid b$  means "a divides b in  $\mathbb{Z}[\sqrt{7}]$ ").

(c) Show that  $(8 + 3\sqrt{7})^d$  is in  $\mathbb{Z}[\sqrt{7}]^\times$  for each  $d \in \mathbb{Z}$ . In other words, show that  $(8 + 3\sqrt{7})^d$  is a **unit** in  $\mathbb{Z}[\sqrt{7}]$  for every integer  $d$ .

8. Let  $D$  be a **dihedral group** of order 8. Draw a **lattice of all subgroups** of  $D$ .

**Linear Algebra.**

1. Let  $A \in \mathbb{C}^{6 \times 6}$ . Assume that

$$\dim \ker(A - 2)^2 = 3 \text{ and } \dim \ker(A - 3)^3 = 2.$$

What are the possible **Jordan normal forms** of  $A$ ?

2. Let  $V$  be a **vector space** with only **finitely many elements**. Compute the **sum of all vectors** in  $V$ .

**Rings and modules.**

3. Give an example of an **integral domain** that is not a **UFD**. (Justify!)
4. Let  $n \in \mathbb{N}$  and let  $p$  be a prime. Let  $V$  be the **vector space** of **univariate polynomials** of degree at most  $n$  with coefficients in  $\mathbb{F}_p$ . We consider  $V$  as an  $\mathbb{F}_p[X]$ -**module** by letting  $X$  act as (formal) **differentiation**,  $X \cdot f = f'$ . Determine the **primary decomposition** of  $V$ .

**Group theory.**

5. Let  $Z(G)$  denote the **centre** of a group  $G$ , and let  $p$  be a **prime**.
- (a) Show that if  $G/Z(G)$  is **cyclic**, then  $G$  is **abelian**.
- (b) Use the **Class Equation** to deduce that every group  $G$  of order  $p^2$  is abelian.
6. Let  $A_n$  denote the **alternating subgroup**— of the **symmetric group**  $S_n$ .
- (a) What is the **maximal order** of an element in  $S_7$ ?
- (b) What is the **maximal order** of an element in  $A_7$ ?

**Field theory.**

7. Let  $F$  be a **finite field** of characteristic  $p$ .
- (a) Prove that  $F$  is **perfect**; that is, every element in  $F$  is a  $p^{\text{th}}$  power in  $F$ .
- (b) Prove that every **irreducible polynomial**  $f$  over  $F$  is **separable**.  
(Hint: *consider  $f'$* .)
8. Find the **Galois group**  $G$  (up to isomorphism) of  $x^6 - 4x^3 + 4 \in \mathbb{Q}[x]$ .

4. SPRING 2018

1. Let  $R$  be a commutative ring with 1 and  $I$  a proper ideal in  $R$ . Show that there exists a minimal prime ideal  $P$  such that  $I \subseteq P$ .
2. Let  $R$  be a commutative ring with 1. Let  $P$  and  $Q$  be prime ideals of  $R$  and suppose that every element of  $R \setminus (P \cup Q)$  is a unit. Show that either  $P$  or  $Q$  is maximal.
3. Let  $\lambda$  be an eigenvalue of an  $n \times n$  complex matrix  $A$  with algebraic multiplicity  $k$ . Show that the matrix  $(A - \lambda I)^k$  is of rank  $n - k$ .
4. For  $\lambda \in \mathbb{R}$ , we define a symmetric bilinear form  $\langle \cdot, \cdot \rangle$  on the space of all  $2 \times 2$  real matrices by
 
$$\langle A, B \rangle = \lambda \cdot \operatorname{tr}(A \cdot B) + \operatorname{tr}(A \cdot B^t),$$
 where  $\operatorname{tr} A$  denotes the trace of a matrix  $A$  and  $A^t$  is the transpose of  $A$ . For which values of  $\lambda \in \mathbb{R}$  is the form  $\langle \cdot, \cdot \rangle$  positive-definite?
5. Let  $G$  be a finite group and  $H$  a subgroup of index  $p$  where  $p$  is the smallest prime dividing the order of  $G$ . Prove that  $H$  is a normal subgroup of  $G$ .
6. Let  $p$  be a prime number and let  $S_p$  be the symmetric group on  $p$  letters. Let  $\tau_p$  be a  $p$ -cycle in  $S_p$ . Determine the size of the normalizer subgroup of  $C_p = \langle \tau_p \rangle$  in  $S_p$ .
7. Determine the Galois group of the polynomial  $f(x) = x^8 - 1$  over the finite field  $\mathbb{F}_3$ .
8. Let  $F, K, L$  be fields where  $K/F$  and  $L/F$  are Galois extensions. Show that the composite  $KL$  is Galois over  $F$  and that  $\operatorname{Gal}(KL/F)$  is isomorphic to the following subgroup of  $\operatorname{Gal}(K/F) \times \operatorname{Gal}(L/F)$ :
 
$$\{(\sigma, \tau) \in \operatorname{Gal}(K/F) \times \operatorname{Gal}(L/F) : \sigma|_{K \cap L} = \tau|_{K \cap L}\}.$$

5. FALL 2017

1. (a) Find a **generator** for the **group of units**  $(\mathbb{Z}/17\mathbb{Z})^\times$ .  
(b) Prove that  $\mathbb{Q}^\times$  is not a **cyclic group**.
2. Explicitly construct a **Sylow 2-subgroup** in the **symmetric group**  $S_6$ .
3. Let  $V$  be a **complex vector space**. Say a **subspace**  $W \subseteq V$  has **finite codimension** if and only if the **quotient space**  $V/W$  has **finite dimension**, that is  $[V : W] = \dim_{\mathbb{C}}(V/W)$  is finite. Let  $W_1, W_2 \subseteq V$  be subspaces.  
(a) Prove: If  $W_1, W_2$  have finite codimension, then  $W_1 \cap W_2$  has finite codimension.  
(b) Show that  $[V : W_1 \cap W_2] = [V : W_1] + [W_1 : W_1 \cap W_2]$ .
4. Let  $V$  be a 2-dimensional, **real vector space**, and  $T : V \rightarrow V$  an **orthogonal linear transformation**. Prove that  $T$  is **diagonalizable** over  $\mathbb{C}$ .
5. Recall that a ring element  $r$  is **nilpotent** if  $r^n = 0$  for some positive integer  $n$ , and **unipotent** if  $r - 1$  is nilpotent. Characterize the nilpotent elements of  $\mathbb{Z}/72\mathbb{Z}$ .
6. Construct three examples each (if possible) of **upper triangular**  $3 \times 3$  real matrices  $A, B, C, D$  satisfying the following. If an example does not exist, briefly explain why.  
(a)  $A$  is **diagonal** and has **characteristic polynomial**  $\lambda^2(\lambda - 1)$ .  
(b)  $B$  has **minimal polynomial**  $\lambda^2(\lambda - 1)$  and **characteristic polynomial**  $\lambda(\lambda - 1)^2$ .  
(c)  $C$  is **orthogonal** but is not a scalar multiple of the identity matrix.  
(d)  $D$  is **nilpotent** and **unipotent**.
7. Let  $F$  be the **splitting field** of  $x^4 + 2x^2 + 2 \in \mathbb{Q}[x]$ . Compute the **Galois group** of the extension  $F/\mathbb{Q}$ .
8. Suppose  $A$  is a **real matrix** with **characteristic polynomial**  $(\lambda^2 + 1)(\lambda^2 + 2)$ . Describe all **real subspaces**  $V \in \mathbb{R}^4$  satisfying  $A(V) \subseteq V$ .
9. Construct the **finite field**  $\mathbb{F}_{5^2}$ , and find an element of the **multiplicative group**  $\mathbb{F}_{5^2}^\times$  which is not a **cube**. Explain why your constructions are valid.

6. SPRING 2017

1. Show that  $\mathbb{Z}[X]$  is not a **principal ideal domain**.
2. Let  $F$  be a field and let  $M$  be an **invertible**  $2 \times 2$  matrix with entries in  $F$ . Suppose that there is a positive integer so that  $M^n = I_2$ . Prove or disprove:  $M$  is **diagonalisable**.
3. Consider the **group homomorphism**

$$\phi: \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$$

given by **left multiplication** by the matrix

$$\begin{bmatrix} 102 & 69 \\ 48 & 33 \end{bmatrix}.$$

What is  $|\text{coker}(\phi)|$ ? (Here  $|X|$  means order (cardinality).)

4. Consider the **ring**  $V = \mathbb{C}[x]/(x^4 + 2x^2 + 1)$ . We can view  $V$  as a **finite dimensional vector space** and multiplication by  $x$  gives a **linear operator**  $V \rightarrow V$ . Find the **Jordan form** of this operator.
5. Let  $G$  be a group of **order**  $p^n$  where  $p$  is a prime and  $n > 0$ . Suppose that  $G$  is **simple**. Show that  $n = 1$ .
6. Let  $R$  be an **integral domain**. Define what it means for  $x \in R$  be **irreducible**. Now suppose that  $x$  is irreducible. Prove or disprove: the ideal  $\langle x \rangle = xR$  is **prime**.
7. Let  $F = \mathbb{Q}(\sqrt{2}) := \{q_1 + q_2\sqrt{2} : q_1, q_2 \in \mathbb{Q}\}$ . Determine which **field extensions**  $F_1/\mathbb{Q}$ ,  $F_2/\mathbb{Q}$ ,  $F_3/\mathbb{Q}$  described below, are **Galois**, and determine their **Galois groups**. Recall that  $F(\alpha)$  means the **smallest field containing  $F$  and  $\alpha$** .
  - (a)  $F_1 = F(\sqrt[4]{2})$ .
  - (b)  $F_2 = F(\sqrt{\sqrt{2} + \sqrt{2}})$ .
  - (c)  $F_3 = F(1 + \sqrt{2})$ .
8. Show that any **group** of **order** 21 contains a **normal cyclic subgroup** of order 7.

Bonus question: Determine **all groups** of order 21.



7. FALL 2016

1. (a) List all **abelian groups** (up to isomorphism) of **order** 200 that have no **elements of order** 40.  
 (b) Explain why the number of **isomorphism classes** of **abelian groups of order**  $p^n$  is independent of the **prime**  $p$ .
2. Let  $p$  be a **prime** number. Assume that  $G$  is a **finite group** such that every element of  $G$  has **order**  $p^n$  for some  $n \geq 0$ . Prove that  $G$  has **order**  $p^N$  for some  $N \geq 0$ . State clearly which theorems (from finite group theory) you use in your proof.
3. (a) Find the **splitting field**  $K$  of the given polynomial  $f$  over  $k$ , in each case, and express your answer in the form  $k(x_1, \dots, x_n)$  for appropriate complex numbers  $\{x_i\}$ .  
 (i)  $f(x) = x^3 - 3$  over  $k = \mathbb{Q}$ .  
 (ii)  $f(x) = x^2 + 3$  over  $k = \mathbb{R}$ .  
 (iii)  $f(x) = x^n + 1$  over  $k = \mathbb{Q}$ .  
 (b) Find the **degree** of each splitting field in (i), (ii) and (iii) and identify the **Galois group**  $G = \text{Gal}(K/k)$  in each case.
4. Let  $k \subseteq K$  be a **finite extension** of fields.  
 (a) Define what it means for  $k \subseteq K$  to be **separable**.  
 (b) Define what it means for  $k \subseteq K$  to be **normal**.  
 (c) Find a finite extension  $L$  of  $\mathbb{Q}$  that is not normal.  
 (d) Does there exist a finite extension field of  $\mathbb{Q}$  that is not separable? Why or why not?
5. Let  $f(x) = x^3 - 2x^2 + 3x - 5$ . Assume that  $f$  has roots  $\alpha, \beta$  and  $\gamma$ . Calculate  $\alpha^2 + \beta^2 + \gamma^2$ .
6. Let  $A$  be an  $n \times m$ -matrix with entries in some field  $F$ .  
 (a) Define what a **reduced row-echelon form** of  $A$  is.  
 (b) Show that the reduced row-echelon form of  $A$  is unique.  
 (Hint: Assume that there are two distinct reduced row-echelon forms and look at the first column where they differ.)
7. Let  $A \in \mathbb{C}^{n \times n}$ . Show that the **Jordan canonical form** of  $A$  has exactly one **Jordan block** per **eigenvalue** if and only if there is no non-zero polynomial  $p \in \mathbb{C}[x]$  of degree less than  $n$  satisfying  $p(A) = 0$ .
8. Let  $R$  be a **commutative ring (with unit)** having only one **maximal ideal**  $\mathfrak{m}$ . Show that any element not in  $\mathfrak{m}$  is **invertible**.
9. Let  $R$  be a **PID**, and  $M$  be a **finitely generated projective module** over  $R$ . Show that  $M$  is **free**.
10. Let  $R$  be a **Noetherian ring**, and let  $M$  and  $N$  be **finitely generated**  $R$ -modules. Show that the  $R$ -module  $\text{Hom}_R(M, N)$  is finitely generated.

8. SPRING 2016

1. Consider a **finite field**  $\mathbb{F}_p$  where  $p$  is a **prime** number. Give necessary and sufficient conditions on  $n$  so that the field extension  $\mathbb{F}_{p^n}/\mathbb{F}_p$  has no **proper subextensions**.

2. Let  $p$  be an **odd prime** and  $n$  be an integer not divisible by  $p$ . The **Legendre symbol** is defined by

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \equiv x^2 \pmod{p} \text{ for some } x \\ -1 & \text{otherwise.} \end{cases}$$

(a) Suppose that  $n$  and  $m$  are not divisible by  $p$ . Show that

$$\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right) \left(\frac{m}{p}\right).$$

(b) Write down the formula for  $\Phi_p(X)$  the  $p$ th **cyclotomic polynomial**. There is no need to prove your formula is correct.

(c) Let  $\zeta \in \mathbb{C}$  be a **primitive**  $p$ th **root of unity**. Show that  $1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0$ .

(d) Show that

$$\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) = 0$$

where  $p$  is an odd prime.

(e) Let  $\zeta$  be a primitive  $p$ th root of unity. Set

$$S = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta^n$$

Show that

$$S^2 = \left(\frac{-1}{p}\right) p.$$

3. Let  $n$  be a positive integer and denote by  $S_{2n}$  the **symmetric group** on  $2n$  letters. Let  $D$  be a **Sylow  $p$ -subgroup** of  $S_{2n}$ . Prove or disprove: there is an integer  $n > 5$  and a prime  $p$  so that  $D$  is isomorphic to a **dihedral group**.

4. Consider the **homomorphism** of  $\mathbb{Z}$ -modules

$$\phi: \mathbb{Z}^3 \rightarrow \mathbb{Z}^2, \quad \phi(\mathbf{x}) = A\mathbf{x}$$

where

$$A = \begin{bmatrix} 3 & 9 & 9 \\ 9 & -3 & 9 \end{bmatrix}.$$

(a) Find a  **$\mathbb{Z}$ -basis**  $\beta = \{\mathbf{v}_1, \mathbf{v}_2\}$  of  $\mathbb{Z}^2$  and positive integers  $d_1 \mid d_2$  such that  $\beta' = \{d_1\mathbf{v}_1, d_2\mathbf{v}_2\}$  is a  $\mathbb{Z}$  basis of  $\text{im}(\phi)$ .

(b) Use the previous part to describe the  $\text{coker}(\phi) = \mathbb{Z}^2/\text{im}(\phi)$  as a direct sum of **cyclic groups**.

5. Let  $V$  be a **vector space** of dimension  $n$  over  $\mathbb{C}$ . In what follows, we will write  $\text{GL}(V)$  for the **group of linear automorphisms** of  $V$  and for  $g \in \text{GL}(V)$ , we write  $|g|$  for its **order** in this group. An element  $g \in \text{GL}(V)$  is called a **pseudo-reflection** if  $g$  has **finite order** (i.e.  $|g| < \infty$ ) and the **1-eigenspace** of  $g$  has dimension  $n - 1$ . In what follows, we will write  $V_g$  for the 1-eigenspace of a pseudo-reflection  $g$ .

(Recall that the 1-eigenspace is the subspace of eigenvectors with eigenvalue 1.)

- (a) Let  $G$  be a **finite subgroup** of  $\text{GL}(V)$  and let  $V^G$  be the subspace of vectors fixed by  $G$ , that is  $v \in V^G$  if and only if  $gv = v$  for every  $g \in G$ . Show that there is a subspace  $W \subseteq V$  such that for every  $g \in G$ ,  $g(W) = W$  and  $W \oplus V^G = V$ .

(Hint: Consider the linear operator  $T: V \rightarrow V$  given by

$$T(v) = \frac{1}{|G|} \sum_{g \in G} gv.$$

Consider the image of  $T$  and its kernel.)

- (b) Give an explicit example to show that there exist pseudo-reflections  $g, h \in \text{GL}(V)$  with  $|g| = |h|$  and  $V_g = V_h$  but  $g$  and  $h$  **do not commute**.
- (c) Suppose that  $g$  and  $h$  are pseudo-reflections with  $V_g = V_h$  and the subgroup of  $\text{GL}(V)$  generated by  $g$  and  $h$  is finite then show that  $g$  and  $h$  **commute**. Further if  $g$  and  $h$  have the same **characteristic polynomial** then show that  $g = h$ .
- (d) Suppose that  $g$  and  $h$  are pseudo-reflections such that  $V_g \neq V_h$  and  $G = \langle g, h \rangle$  is **finite**. If for any other pseudo-reflection  $k \in \langle g, h \rangle$  we have  $V_k = V_g$  or  $V_k = V_h$  then show that  $g$  and  $h$  commute. (Here,  $\langle g, h \rangle$  is the subgroup of  $\text{GL}(V)$  generated by  $g$  and  $h$ .)
6. Let  $V$  be a complex vector space with a **positive-definite Hermitian form**  $\langle v, w \rangle$ . Let  $T$  be a **self-adjoint operator** on  $V$ .
- (a) Show that every **eigenvalue** of  $T$  is **real**.
- (b) Let  $v$  and  $v'$  be **eigenvectors** of  $T$  with **distinct eigenvalues**  $\lambda$  and  $\lambda'$  respectively. Show that  $v$  and  $v'$  are **orthogonal**.
- (c) Give an example of a self-adjoint operator  $T$  and **two distinct non-orthogonal eigenvectors**  $v$  and  $v'$ .
7. Let  $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$ .
- (a) Find a **splitting field**  $K$  of  $f$  over  $\mathbb{Q}$  and the **degree**  $[K : \mathbb{Q}]$ .
- (b) Determine the **Galois group** of  $f$  over  $\mathbb{Q}$ . Determine the **action** of the generator(s) of the Galois group explicitly on the roots of  $f$ .
8. Let  $F, L, M, K$  be **fields** with  $F \subset L \subset K$  and  $F \subset M \subset K$ . Assume that  $[L : F] < \infty$  and  $[M : F] < \infty$ .
- (a) Let  $\{m_1, \dots, m_k\}$  be a basis of  $M$  as an  $L \cap M$  vector space. Show that  $E = \sum_{i=1}^k LM_i$ , the  $L$ -subspace of  $K$  spanned by  $\{m_1, \dots, m_k\}$  is a subfield of  $K$  containing both  $L$  and  $M$ .
- (b) Explain why (a) implies that  $[LM : L] \leq [M : L \cap M]$ .
- (c) Use (a) to show that  $[LM : F] = [L : F][M : F]$  implies that  $L \cap M = F$ .  
(Hint: draw a picture of all fields involved, including  $L \cap M$ !)
- (d) Let  $F = \mathbb{Q}$  and  $K = \mathbb{C}$ . Let  $\alpha$  be a **real cube root** of 2 and  $\beta$  a **complex cube root** of 2 and let  $L = \mathbb{Q}(\alpha)$  and  $M = \mathbb{Q}(\beta)$ . Carefully justify that  $[LM : F] < [L : F][M : F]$  in this case.

9. FALL 2015

1. Let  $A$  be an  $n \times n$  matrix with  $n$  **distinct complex eigenvalues**, for an integer  $n \geq 1$ . Let  $\text{Mat}_{n \times n}$  be the **vector space of  $n \times n$  matrices** over  $\mathbb{C}$ . Consider the **linear operator**  $T_A: \text{Mat}_{n \times n} \rightarrow \text{Mat}_{n \times n}$  given by  $T_A(X) = AX - XA$ . What is **dim image  $T_A$** ?  
(Hint: *What is  $\ker T_A$ ?*)
2. Find all **abelian groups**  $G$ , up to isomorphism, with the property that  $G$  **has a subgroup**  $H \simeq \mathbb{Z}/4\mathbb{Z}$  for which  $G/H \simeq \mathbb{Z}/8\mathbb{Z}$ .
3. (a) Show that the **group of units** in the ring  $\mathbb{Z}/8\mathbb{Z}$  is **not cyclic**.  
(b) Show that, if  $p$  is **prime**, then the group of units in  $\mathbb{Z}/p\mathbb{Z}$  is **cyclic**.
4. Let  $F$  be a field, and let  $G = \text{GL}_2(F)$ , the **group of invertible  $2 \times 2$  matrices** with entries in  $F$ . Suppose  $A \in G$  is an **element of finite order  $k$** , for some  $k \geq 1$ .  
(a) Suppose  $F = \mathbb{C}$ . Show that  $A$  is **diagonalizable**.  
(b) Suppose  $F = \mathbb{R}$ . Show that  $A$  **need not be diagonalizable** by giving a counterexample.  
(c) Suppose  $F = \overline{\mathbb{F}}_2$ , an algebraically closed field of characteristic 2. Must  $A$  be diagonalizable? Prove or disprove.
5. Suppose that  $a$  and  $b$  are **relatively prime** elements in a **Unique Factorization Domain**  $R$ . Show that there are no **nonzero  $R$ -module homomorphisms**  $f: R/(a) \rightarrow R/(b)$ .
6. Let  $p$  be a **prime**. Show that any group  $G$  of order  $p^2$  is **abelian**.
7. Show that no **group of order 30** is **simple**.
8. Show that the **additive group**  $\mathbb{Q}$  is **not isomorphic** to the **product** of two non-trivial groups.
9. Let  $F$  be a **subfield** of  $\mathbb{R}$ , and let  $f(X) \in F[X]$  be **irreducible** with a **non-real root**  $\alpha$  of absolute value one. Show that  $1/\beta$  is a root of  $f(X)$  for every root  $\beta \in \mathbb{C}$  of  $f(X)$ .
10. Let  $E/F$  be a **field extension**. Let  $f(X) \in F[X]$  be **irreducible** and  $\alpha_1, \alpha_2, \beta_1, \beta_2 \in E$  be **roots** of  $f(X)$ . Assume  $\alpha_1 \neq \alpha_2, \beta_1 \neq \beta_2$ .  
(a) Show that  $F(\alpha_1)$  and  $F(\alpha_2)$  are **isomorphic extensions** of  $F$ .  
(b) Are  $F(\alpha_1, \alpha_2)$  and  $F(\beta_1, \beta_2)$  always isomorphic extensions of  $F$ ?
11. Let  $E$  be the **splitting field** of  $f(X) = X^4 - 14X^2 + 9$  over  $\mathbb{Q}$ .  
(a) Compute  $\text{Gal}(E/\mathbb{Q})$ .  
(Hint: *The roots of  $f(X)$  are  $\pm\sqrt{2} \pm \sqrt{5}$* )  
(b) Verify that each **subgroup** of  $\text{Gal}(E/\mathbb{Q})$  is the **Galois group**  $\text{Gal}(E/L)$  of an **intermediate field**  $\mathbb{Q} \subseteq L \subseteq E$ .
12. Let  $R$  be a **commutative ring with 1**,  $N$  a **nilpotent** ideal of  $R$ , and  $\pi: R \rightarrow R/N$  the **quotient** map.  
(a) Prove that if  $\pi(r)$  is a **unit** (invertible element) in  $R/N$ , then  $r$  is a unit in  $R$ .  
(b) Prove that the induced map from  $\text{GL}_n(R)$  to  $\text{GL}_n(R/N)$  is **surjective**.  
(Hint: *Recall that  $\text{GL}_n(R)$  denotes the **group of invertible  $n \times n$  matrices** over  $R$ .*)

13. Let  $k$  be a field.

- (a) Prove that the polynomial ring  $k[t]$  is a principal ideal domain.
- (b) Suppose that  $I_1 \subseteq I_2 \subseteq \cdots$  is an ascending chain of ideals in a principal ideal domain  $R$ . Prove that there is a number  $N$  such that  $I_N = I_{N+1} = \cdots$ .
- (c) Prove that every element of a principal ideal domain  $R$  is a product of irreducible elements.

14. Let  $R$  be an integral domain with field of fractions  $F$ .

- (a) Define what it means for an element  $a$  of  $F$  to be integral over  $R$ .
- (b) Define what it means for  $R$  to be integrally closed.
- (c) Show that a unique factorization domain is integrally closed.

10. SPRING 2015

1. Let  $(V, \langle \cdot, \cdot \rangle)$  be an **inner product space** over  $\mathbb{C}$ , and let  $T: V \rightarrow V$  be a **linear operator**.

- (a) Define the **adjoint**  $T^*: V \rightarrow V$  (just say how it is defined, not why it exists).
- (b) Suppose that  $W \subseteq V$  is a  **$T$ -invariant subspace**. Show that  $W^\perp$  is  $T^*$ -invariant.
- (c) Show that if  $\lambda$  is an **eigenvalue** of  $T$  then  $\bar{\lambda}$  is an **eigenvalue** of  $T^*$ .

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

- (a) Find the **characteristic polynomial** of  $A$ .
- (b) Find  $E_\lambda$  (the **eigenspace** of  $\lambda$ ) for each **eigenvalue**  $\lambda$  of  $A$ .
- (c) Find the **Jordan canonical form** of  $A$ .

3. Let  $A = \begin{pmatrix} 4 & 3 & 5 \\ 2 & 4 & 2 \\ 3 & 1 & 3 \end{pmatrix}$ . Find  $d_1, d_2, d_3 \in \mathbb{Z}$  such that  $d_1 | d_2 | d_3$  and  $A$  is **equivalent** to  $D = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}$ .

4. Examples and counter-examples.

- (a) Give an example of a **U.F.D.** that is not a **P.I.D.**
- (b) Give an example of a **linear transformation**  $\alpha: V \rightarrow V$  over a **field**  $k$  such that  $V$  is **cyclic** as a  $k[x]$ -**module**, but decomposable as a  $k[x]$ -**module**.
- (c) Let  $a = 3 + 4i, b = 1 + 2i \in \mathbb{Z}[i]$ . Write

$$a = bq + r$$

where  $r, q \in \mathbb{Z}[i]$ , and  $N(r) < N(b) = 5$ . (Here  $N(a + bi) = a^2 + b^2$  is the **complex norm**.)

5. Let  $V$  be an  $n$ -**dimensional vector space** over  $\mathbb{C}$  and let  $f: V \rightarrow V$  be a **linear transformation**. Prove that there exists a **basis**  $B = \{v_1, \dots, v_n\}$  of  $V$  such that  $f$  is in **upper-triangular** form with respect to  $B$ .

- 6. (a) Let  $A$  be a **commutative ring** with  $1 \in A$ . Prove that  $A$  has a **maximal proper ideal**  $M$ .
- (b) Prove that the **rings**  $F[x, y]/(y^2 - x)$  and  $F[x, y]/(y^2 - x^2)$  are not **isomorphic** over any **field**  $F$ .

- 7. (a) Show that the polynomial  $f(x) = x^4 - 5$  is **irreducible** over  $\mathbb{Q}$ .
- (b) Find the **splitting field**  $K$  of  $f(x)$  over  $\mathbb{Q}$ .
- (c) Find the **Galois group** of  $K/F$ .

8. Let  $p$  be a **prime number** and  $\mathbb{F}_p$  be a **field** with  $p$  elements. Let  $\text{GL}_4(\mathbb{F}_p)$  be a group of **invertible matrices** over  $\mathbb{F}_p$  of size 4 by 4, and let  $U_4(\mathbb{F}_p)$  be an **upper triangular subgroup** of  $\text{GL}_4(\mathbb{F}_p)$  with all diagonal elements equal to 1. Show that  $U_4(\mathbb{F}_p)$  is a  **$p$ -Sylow subgroup** of  $\text{GL}_4(\mathbb{F}_p)$ .

9. Let  $p$  be a prime number and let  $\mathbb{F}_p$  be a **field** with  $p$ -elements. Determine the number of quadratic **monic irreducible polynomials** over  $\mathbb{F}_p$ . (A **monic polynomial** means that its leading coefficient is 1.)

10. Let  $G$  be a **group** with 21 elements. Show that:
- $G$  has a unique **Sylow subgroup**  $P$  of order 7.
  - $P$  is a **normal subgroup** of  $G$  and there exists an element  $\sigma \in G$  such that  $\sigma \neq 1$  and  $\sigma^3 = 1$ .
  - Assume that  $G$  as above, is **not cyclic**. Show that  $G$  is a **semi-direct product**  $G = P \rtimes \{1, \sigma, \sigma^2\}$  where  $P = \{1, y, \dots, y^6\}$  and  $\sigma\tau\sigma^{-1} = y^2$ , or  $\sigma\tau\sigma^{-1} = y^4$ .
  - Show that both groups  $G$  described in (c) are **isomorphic**.
11. (a) Show that if in a group  $G$  we have  $\sigma^2 = 1$  for all  $\sigma \in G$ , then  $G$  is **abelian**.
- (b) Let  $p$  be an odd prime number and let  $\mathbb{F}_p$  be a **field** with  $p$ -elements. Consider the group  $G = U_3(\mathbb{F}_p)$ . This means that  $G$  is a group of all  $3 \times 3$  **upper triangular invertible matrices** over  $\mathbb{F}_p$  with diagonal elements all equal to 1. Show that  $\sigma^p = 1$  for all  $\sigma \in G$ , but  $G$  is not an **abelian group**.
12. Decide which of the following extensions of  $\mathbb{Q}$  are **Galois extensions** of  $\mathbb{Q}$ , and explain your answer carefully.
- $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ .
  - $\mathbb{Q}(\sqrt{2}, \sqrt{-1})(\sqrt{1 + \sqrt{2}})/\mathbb{Q}$ .
  - $\mathbb{Q}(\sqrt{2}, \sqrt{-1})/\mathbb{Q}$ .
  - $\mathbb{Q}(\sqrt{7})(\sqrt{1 + \sqrt{7}})/\mathbb{Q}$ .

11. FALL 2014

1. Does there exist a **finite abelian group** of order 16 with 4 elements of order 4? If such a group  $M$  exists, we know that  $M$  is **isomorphic** to a group of the form

$$\mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z},$$

where  $m_1 \geq m_2 \geq \cdots \geq m_k$ . What are  $k$  and  $m_i$ , and are they unique?

2. Show that every non-zero **prime ideal** in a **principal ideal domain**  $R$  is in fact a **maximal ideal**.
3. Let  $p$  be a **prime** number. Let  $K/\mathbb{F}_p$  be a **finite Galois extension**. The purpose of this problem is to show that  $\text{Gal}(K/\mathbb{F}_p)$  is **cyclic**.

- (a) Show that the function  $F: K \rightarrow K$  given by  $F(x) = x^p$  is in fact a **homomorphism**.
- (b) Show that  $F$  is an **automorphism** fixing  $\mathbb{F}_p$ .
- (c) Suppose that the order of  $F$  is  $n$  in  $\text{Gal}(K/\mathbb{F}_p)$ . Show that the polynomial  $X^{p^n} - X$  vanishes on  $K$ .
- (d) Conclude that  $\text{Gal}(K/\mathbb{F}_p)$  is **cyclic** of order  $n$ .

4. Consider the  $n \times n$  **real matrix**

$$B = \begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & n-1 \end{pmatrix}$$

In other words  $B$  is a **diagonal matrix** with **eigenvalues**  $-1, 1, 2, \dots, n-1$ . Show that there is no real matrix  $A$  with  $A^2 = B$ .

5. Show that the **extension**  $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$  is **Galois** of degree 4. Compute its **Galois group**, and make sure you completely justify your answer.

6. Let  $N$  be an  $n \times n$  **complex matrix** with  $N^n = 0$ . Show that  $\det(I_n + N) = 1$ .

7. Let  $p$  be a **prime** number.

- (a) What is a **Sylow  $p$ -subgroup** of a finite group  $G$ ?
- (b) State, but do not prove, the **Sylow theorems**.
- (c) Find a **Sylow 2-subgroup** of  $S_4$ .

8. Let  $f: \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$  be the **homomorphism** of **abelian groups** given by

$$f(v) = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} v,$$

for  $v \in \mathbb{Z}^2$ . Describe  $\ker(f)$  and  $\text{coker}(f)$  up to isomorphism as **direct sums of cyclic groups**. (Recall  $\text{coker}(f) := \mathbb{Z}^2 / \text{im}(f)$ .)

9. (a) Prove that a  $n \times n$  **matrix over  $\mathbb{C}$**  satisfying  $A^3 = I_3$  can be **diagonalized**.
- (b) Find a **field  $k$**  and a  $3 \times 3$  matrix  $A$  satisfying  $A^2 = I_3$  that cannot be **diagonalized**.

10. Show that any **group of order 14** is **isomorphic** to either a **cyclic** or a **dihedral group**.



11. Let  $f \in \mathbb{Q}[x]$  be an **irreducible polynomial** of degree 4. Let  $L$  be the **splitting field** of  $f$  and suppose that  $[L : \mathbb{Q}] = 8$ . Prove or disprove: the group  $G = \text{Gal}(L/\mathbb{Q})$  is not abelian.

12. Suppose  $M$  and  $N$  are  **$R$ -modules** and  $I$  and  $J$  are **ideals** for which

- $MI = 0$  and  $JN = 0$ ;

- $I + J = R$ .

Prove that  $M \otimes_R N = 0$ .

12. SPRING 2014

1. Find all **finite abelian groups**  $G$  with  $|\text{Aut}(G)|$  a **prime** number.
2. Let  $p$  be a **prime** number,  $S_p$  the **symmetric group** on  $p$  letters,  $\sigma \in S_p$  a  $p$ -cycle and  $\tau \in S_p$  a **transposition**. Show that  $\sigma$  and  $\tau$  generate  $S_p$ . Justify your answer carefully.
3. Let  $F$  be a **finite field** of **characteristic**  $p$ , and  $G$  a subgroup of order  $p^a$ ,  $a \in \mathbb{N}$  of the group  $\text{GL}(n, F)$ . Show that there is a nonzero vector  $\mathbf{v}$  of  $F^n$  such that  $g\mathbf{v} = \mathbf{v}$  for all  $g \in G$ .
4. Let  $f(x) \in F[X]$  be an **irreducible polynomial** of degree  $d$  over a **field**  $F$ . Let  $K/F$  be a **finite field extension** of degree  $n$ . Show that if  $\gcd(n, d) = 1$ , then  $f(x)$  is **irreducible** as a polynomial in  $K[X]$ .
5. Determine the **Galois group** of  $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ . Justify your answer.  
(Hint: *you may use Question 2 here, even if you haven't solved it.*)
6. Show that the identity map is the only **field automorphism** of the real numbers. Show that this is not true for the complex numbers.  
(Hint: *show that  $a < b$  implies  $\sigma(a) < \sigma(b)$  for any  $a, b \in \mathbb{R}$  and any **field automorphism**  $\sigma$  of  $\mathbb{R}$ .)*
7. Let  $V$  be an  $n$ -**dimensional vector space** over an **algebraically closed field**  $F$ , and let  $T : V \rightarrow V$  be a **linear map**. Show that there exists a **basis**  $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$  for  $V$  such that the matrix of  $T$  with respect to  $B$  is **upper triangular**. Find a counterexample over a **non-algebraically closed field**.
8. Let  $A \subset M_{nn}(\mathbb{R})$  be a **subspace** of pairwise commuting **symmetric matrices**. Show that  $\dim(A) \leq n$ .
9. Let  $V$  be a **finite-dimensional vector space** over a **field**  $F$ . Find all (one-sided) **zero-divisors** in the **ring**  $\text{End}_F(V)$  of linear maps  $V \rightarrow V$ . Justify your answer.
10. Let  $R = \mathbb{Z}[T, T^{-1}]$  be the **ring of Laurent polynomials** in one variable.
  - (a) Show that the **units** in  $R$  are  $R^\times = \{\pm T^n : n \in \mathbb{Z}\}$ .
  - (b) Find all **ring homomorphisms**  $f : R \rightarrow R$ .
11. Let  $A$  be a **commutative ring** (with identity element). Show that if  $A$  has finite cardinality, then every **prime ideal** of  $A$  is **maximal**.
12. Let  $A$  be a **commutative ring** (with identity element) and let  $I \triangleleft A$  be a **nilpotent ideal** of  $A$ . That is, there exists  $k \in \mathbb{N}$  such that  $I^k = 0$ . Let  $\pi : A \rightarrow A/I$  be the canonical projection. Show that  $a \in A$  is **invertible** in  $A$  if and only if  $\pi(a)$  is **invertible** in  $A/I$ .

13. FALL 2013

1. (a) Let  $A$  and  $B$  be  $5 \times 5$  matrices over  $\mathbb{C}$  with the same **minimal polynomial** and **characteristic polynomial**, and with at least three distinct **eigenvalues**. Prove that  $A$  and  $B$  are **similar**.  
 (b) Find an example of two  $5 \times 5$  matrices  $A$  and  $B$  over  $\mathbb{C}$  which are not **similar** but which have the same **minimal polynomial** and **characteristic polynomial** and **two distinct eigenvalues**.
2. Let  $T$  be a **linear operator** on a **finite-dimensional vector space**  $V$  over a **field**  $k$ . Prove that there exists a **decomposition**  $V = X \oplus Y$  with  $X$  and  $Y$   **$T$ -invariant**, such that  $T|_X : X \rightarrow X$  is **invertible** and  $T|_Y : Y \rightarrow Y$  is **nilpotent**. [note: same as Fall 2004 Question 2]
3. (a) Define the **trace**  $\text{tr}(A)$  of an  $n \times n$  matrix  $A$ , and prove that  $\text{tr}(AB) = \text{tr}(BA)$  for all  $n \times n$  matrices  $A$  and  $B$ .  
 (b) For an  $n \times n$  matrix  $A$  over  $\mathbb{C}$ , show that  $\text{tr}(A)$  is equal to the sum of the **eigenvalues** of  $A$  (repeated according to **multiplicity**).  
 (c) Show that if  $A$  is an  $n \times n$  matrix and  $\text{tr}(AX) = 0$  for all  $n \times n$  matrices  $X$ , then  $A = 0$ .
4. (a) State the **classification of finite abelian groups**.  
 (b) List all **abelian groups of order**  $16 \cdot 9 = 144$ .
5. Let  $H$  be a **subgroup** of a group  $G$  with **normalizer**  $N_G(H) = \{x \in G \mid x^{-1}Hx = H\}$  in  $G$ .  
 (a) Prove that  $|\{x^{-1}Hx \mid x \in G\}| = [G : N_G(H)]$ , assuming that  $N_G(H)$  has **finite index** in  $G$ .  
 (b) Prove that if  $H$  has **finite index** in  $G$ , then  $H$  contains a subgroup  $M$  which is of finite index and **normal** in  $G$ .  
 (c) Prove that if  $H$  is a **proper subgroup** of a finite group  $G$ , then  $\cup_{x \in G} x^{-1}Hx$  is not the whole of  $G$ .
6. Recall that  $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})$  is the **group of  $2 \times 2$  matrices of determinant 1**, which have entries in  $\mathbb{Z}/p\mathbb{Z}$ .  
 (a) Show that the **order** of  $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})$  is  $p(p-1)(p+1)$ .  
 (b) Determine the **number of 5-Sylow subgroups** of  $\text{SL}_2(\mathbb{Z}/5\mathbb{Z})$ .
7. (a) Define what it means for a complex number to be an **algebraic integer**.  
 (b) If  $y$  is an **algebraic integer**, show that for some  $n$  there exists an  $n \times n$  matrix  $A$  with entries in  $\mathbb{Z}$  such that  $AY = yY$ , where  $Y = [1, y, y^2, \dots, y^{n-1}]^t$ .  
 (c) Prove that  $y$  is an **algebraic integer** if and only if it is an **eigenvalue** of a square matrix with entries in  $\mathbb{Z}$ .
8. Let  $R$  be a **commutative ring with unity** that is not a **field**.  
 (a) Prove that the following conditions are equivalent.  
 (i) The sum of two **non-units** is a non-unit.  
 (ii) The non-unit elements form a **proper ideal**.  
 (iii) The ring possesses a unique **maximal ideal**.  
 (b) Show that  $R = k[[x]]$ , where  $k$  is a **field**, is an example of such a **ring**.

9. Let  $R$  be a nontrivial commutative ring with unity, and let  $M$  be a free  $R$ -module with finite basis  $X = \{x_1, \dots, x_m\}$ .
- (a) Prove that every basis of  $M$  is finite.
  - (b) Use Zorn's Lemma to show that  $R$  has a maximal ideal  $J$ .
  - (c) Prove that every basis of  $M$  has  $m$  elements.
10. Let  $F = \mathbb{Q}(\sqrt[4]{2})$  and  $K = \mathbb{Q}(\sqrt[4]{2}, i)$ .
- (a) Show that the extension of  $K$  over  $\mathbb{Q}$  is Galois and compute its Galois group  $G$ . Explain fully.
  - (b) Describe the subgroup  $H$  of  $G$  corresponding to  $F$ .
  - (c) Deduce from part (b) that there is one and only one intermediate field between  $F$  and  $\mathbb{Q}$ .

14. SPRING 2013

1. (a) State the three **Sylow Theorems**.  
 (b) Use these results to prove that any group of order 65 is **cyclic**.
2. Let  $G$  be a **finite group of order  $p^n$  acting on a finite set  $X$** . Prove that
 
$$|X| \equiv |X^G| \pmod{p}$$
 where  $X^G = \{x \in X \mid gx = x \text{ for all } g \in G\}$ .
3. (a) Define what it means for a group  $G$  to be **solvable**.  
 (b) Prove that a group  $G$  of **invertible, upper-triangular matrices** over the **field  $k$**  is solvable.
4. Let  $\mathfrak{m}$  be a **maximal ideal** in  $\mathbb{Z}[X]$ , Prove that  $\mathfrak{m}$  is not a **principal ideal** of  $\mathbb{Z}[X]$ .
5. Consider the **ring  $\mathbb{Z}[X]$  of polynomials** over  $\mathbb{Z}$ .  
 (a) Define what it means for  $f \in \mathbb{Z}[X]$  to be **primitive**.  
 (b) Prove that if  $f \in \mathbb{Z}[X]$  and  $g \in \mathbb{Z}[X]$  are both primitive then  $fg \in \mathbb{Z}[X]$  is also primitive.
6. Let  $n > 1$  and let  $\mathbb{Z}_n$  be the **ring of integers modulo  $n$** .  
 (a) Identify the **units  $\mathbb{Z}_n^*$**  of  $\mathbb{Z}_n$ .  
 (b) Find a formula for the **cardinality  $|\mathbb{Z}_n^*|$** , of  $\mathbb{Z}_n^*$ , in terms of  $n$ .  
 (c) Does there exist an  $n$  such that  $|\mathbb{Z}_n^*| = 14$ ? Why or why not?
7. Let  $V$  be the **real vector space of functions  $f: \mathbb{R} \rightarrow \mathbb{R}$  spanned by  $\beta_0 = \{e^x, e^{-x}, xe^x, xe^{-x}\}$** . Let  $T: V \rightarrow V$  be the **linear mapping** given by  $T(f) = f'$ . Find the **Jordan canonical form  $J$**  of  $T$  and a **basis  $\beta$**  of  $V$  such that the **matrix** of  $T$  with respect to  $\beta$  is  $J$ .
8. Let  $P_n(\mathbb{R})$  be the **real vector space of polynomials of degree at most  $n$** . Let  $T: P_n(\mathbb{R}) \rightarrow P_n(\mathbb{R})$  be defined by  $T(f(x)) = f(-x)$ . Give  $P_n(\mathbb{R})$  the **inner product**

$$\langle f, g \rangle = \int_{-1}^1 f(t)g(t) dt.$$
 (a) Find the **minimal polynomial** of  $T$ , the **eigenvalues** of  $T$  and a description of each **eigenspace**.  
 (b) Prove carefully that  $T$  is **self-adjoint**. Is  $T$  **orthogonally diagonalisable, normal, orthogonal**? Justify each answer.
9. Let  $\theta_7 \in \mathbb{C}$  be a **primitive 7-th root of unity**. What is the **minimal polynomial** of  $\theta_7 + \theta_7^{-1}$  over  $\mathbb{Q}$ ? Justify your answer.
10. Prove that the **centre** of the **ring of  $n$  by  $n$  matrices over a field  $F$**  is  $\{aI_n : a \in F\}$  where  $I_n$  is the  $n$  by  $n$  **identity**.
11. Let  $f(x) = x^4 - 2x^2 - 2 \in \mathbb{Q}[X]$ ,  
 (a) Show that  $f(x)$  is **irreducible** over  $\mathbb{Q}$ .  
 (b) Find the **splitting field  $L$**  of  $f$  over  $\mathbb{Q}$  and its **degree** over  $\mathbb{Q}$ .  
 (c) Find **generators and relations** for the **Galois group** of  $L/\mathbb{Q}$ .
12. Let  $A \in M_{nn}(\mathbb{C})$  have **rank 1**. Show that  $\det(A + I) = \det(A) + 1$ .

1. Let  $U$  be a **unitary matrix** ( $U^*U = UU^* = I$ ). Show that

$$\lim_{n \rightarrow \infty} \frac{I + U + U^2 + \cdots + U^n}{n} = P,$$

where  $P$  is the **orthogonal projection** onto the **subspace**  $\ker(I - U)$ .

(Hint: use the fact that  $U$  is **diagonalizable** in an **orthonormal basis** and consider various **eigenspaces** of  $U$ .)

2. Let  $\text{GL}_n(\mathbb{F}_q)$  denote the **group** of **invertible**  $n$  by  $n$  matrices over a **finite field** with  $q$  elements. Find the number of elements in this group.
3. The **center** of an **algebra**  $A$  is the set of all  $a \in A$  such that  $ab = ba$  for all  $b \in A$ . Determine the center of  $M_{nn}(F)$ , the algebra of  $n$  by  $n$  matrices over a **field**  $F$ .
4. The **exponential map**  $\exp: M_n(\mathbb{C}) \rightarrow \text{GL}_n(\mathbb{C})$ , from complex matrices to **invertible** ones, is defined by

$$\exp(A) = \sum_{p=0}^{\infty} \frac{A^p}{p!}$$

- (a) Show that for any **invertible** matrix  $g$  and any matrix  $A$ , we have

$$\exp(gAg^{-1}) = g \exp(A)g^{-1}$$

- (b) Use (a) to show that any **invertible** matrix with distinct **eigenvalues** is the exponential of a matrix.
- (c) Show that if  $u$  is a **nilpotent matrix** then  $I - u$  is in the range of the exponential map and use this to show that the exponential map is **surjective**.

(Hint: for the very last part you can use the **Jordan canonical form theorem**.)

5. The  **$n$ -th cyclotomic polynomial** is defined as

$$\varphi_n(x) := \prod (x - \zeta_n)$$

where the product is taken over the set of **primitive  $n$ th roots of unity**. (Recall that  $\zeta_n$  is a **primitive  $n$ th root** of 1 iff  $\zeta_n^n = 1$  but  $\zeta_n^i \neq 1$  for all  $i \in \mathbb{N}, i < n$ .) Thus for example  $\varphi_1(x) = x - 1, \varphi_2(x) = x + 1, \varphi_4(x) = x^2 + 1, \dots$  Show that:

(a)  $x^n - 1 = \prod_{d|n} \varphi_d(x)$ .

(b) Deduce from (a) that  $\varphi_n(x) \in \mathbb{Z}[x]$ .

6. Let  $d \mid n, d \neq n$ . Show that  $\varphi_n(x)$  divides the polynomial  $\frac{x^n - 1}{x^d - 1}$  in  $\mathbb{Z}[x]$ .

(Hint: factor the polynomials  $x^n - 1, x^d - 1$  in  $\mathbb{C}[x]$ .)

7. Show that a **group** of order 75 has a **normal Sylow subgroup**.

8. Let  $\omega = \frac{-1}{2} + \frac{\sqrt{-3}}{2}$ . Show that

(a)  $\omega^3 = 1$

(b) The **field extension**  $\mathbb{Q}(\omega, \sqrt[3]{5})$  is a **Galois extension** of  $\mathbb{Q}$ .

(c) Determine the **Galois group**  $\text{Gal}(\mathbb{Q}(\omega, \sqrt[3]{5})/\mathbb{Q})$ .

9. Let  $R$  be a **commutative ring** with unity. Let  $I$  and  $J$  be **ideals** in  $R$  such that  $I + J = R$ . ( $I$  and  $J$  are called **coprime ideals**.) Show that there is a natural **ring isomorphism**

$$\frac{R}{I \cap J} \rightarrow \frac{R}{I} \oplus \frac{R}{J}$$

(This is an abstract form of the **Chinese remainder theorem**).

16. SPRING 2011

Let  $\mathbb{C}^{n \times n}$  denotes the ring of complex  $n \times n$ -matrices.

1. Let  $A \in \mathbb{C}^{n \times n}$ . How can one read off the **degree** of the **minimal polynomial** of  $A$  from the **Jordan canonical form** of  $A$ ?
2. Consider a **(two-sided) ideal**  $I \in \mathbb{C}^{n \times n}$ . Show that  $I = 0$  or  $I = \mathbb{C}^{n \times n}$ .
3. Let  $V$  be a **finite-dimensional  $\mathbb{Q}$ -vector space**, and  $A: V \rightarrow V$  a **linear map** such that  $A^5 = \text{id}_V$ . Assume further that  $A$  has no **fixed point** apart from  $0 \in V$ . Prove that  $\dim(V)$  is **divisible** by 4.
4. Determine all  $n$  such that the **ring  $\mathbb{Z}_n$**  has exactly 12 **invertible elements**.
5. Given an example of a **free module**  $M$  over some **commutative ring**  $R$  and a **submodule**  $N \subseteq M$  that is **torsion-free** but not **free**. (Justify why  $N$  is not free.)
6. Let  $R$  be an **integral domain**.
  - (a) Define the **field of fractions**  $\text{Quot}(R)$  of  $R$  and the canonical **morphism**  $\phi_R: R \rightarrow \text{Quot}(R)$ .
  - (b) When is  $\phi_R$  an **isomorphism**? (Justify!)
7. Let  $G$  be a **group** and  $H \triangleleft G$ . Show that if  $H$  and  $G/H$  are **soluble**, then so is  $G$ .
8. Show that any **group of order 91** is **cyclic**.
9. Determine the **number of conjugacy classes** in the **symmetric group**  $S_5$  and the **number of elements** in each class.
10. Let  $F$  be a field and  $G$  be a **finite subgroup** of the **multiplicative group**  $F \setminus \{0\}$ . Show that  $G$  is **cyclic**.
11. State and prove **Eisenstein's irreducibility criterion**.
12. Let  $p$  be a **prime**, and let  $m$  and  $n$  be two positive integers such that  $m$  divides  $n$ .
  - (a) Explain why  $\mathbb{F}_{p^m}$  is a **subfield** of  $\mathbb{F}_{p^n}$ .
  - (b) Compute  $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ .

1. Find all **ring homomorphisms**  $f: \mathbb{Z} \rightarrow \mathbb{Z}/18\mathbb{Z}$ .
2. For  $n \geq 2$ , characterize the  $n \times n$  **matrices over  $\mathbb{C}$**  which **commute** only with **diagonalisable** matrices.
3. Show that any **group of order 10** is either a **cyclic** group or a **dihedral** group.
4. (a) Let  $G$  be a group. Show that the **conjugation homomorphism**  $c: G \rightarrow \text{Aut}(G)$  is injective if and only if the centre of  $G$  is trivial.
 

(b) If  $G$  is **simple** and **nonabelian**, is  $c$  necessarily an **isomorphism**? Prove or give a counterexample.
5. Suppose that  $A$  and  $B$  are  $4 \times 4$  **matrices over  $\mathbb{C}$**  with the same **minimal polynomial**, **characteristic polynomial**, and at least two **distinct eigenvalues**. Prove that  $A$  and  $B$  are **similar**. Find an example of two  $5 \times 5$  matrices over  $\mathbb{C}$  with the same properties that are not similar.
6. Let  $R$  be an **integral domain**. For an  **$R$ -module**  $M$ , let  $M^* = \text{Hom}_R(M, R)$ .
 

(a) Verify that the function  $i_M: M \rightarrow M^{**}$  given by
 
$$i_M(m)(f) = f(m)$$
 for  $m \in M$  and  $f \in M^*$  is an  **$R$ -module homomorphism** for any  $M$ .

(b) Show that  $i_M$  is injective if and only if  $M$  is **torsion-free**. (Assume  $M$  is finitely generated here).

(c) If  $R$  is a **PID**, show that  $i_M$  is an isomorphism if  $M$  is **torsion-free**.

(d) Give an example of a ring  $R$  and an  $R$ -module  $M$  for which  $i_M = 0$ .

(e) Give an example of a ring  $R$  and an  $R$ -module  $M$  for which  $i_M$  is injective but not surjective.
7. Show that, for positive integers  $m, n$ ,
 
$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$$
 as **abelian groups**, where  $d = \text{gcd}(m, n)$ .
8. Let  $G$  be a finite **group of order**  $504 = 2^3 \cdot 3^2 \cdot 7$ .
 

(a) Show that  $G$  cannot be **isomorphic** to a subgroup of the **alternating group**  $A_7$ .

(b) If  $G$  is **simple**, determine the **number of Sylow 3-subgroups**.
9. Let  $E$  be a **splitting field** of  $x^3 - 2$  over the rationals  $\mathbb{Q}$  and assume that  $E$  is a **subfield** of  $\mathbb{C}$ . Let  $F = E \cap \mathbb{R}$  be the **real subfield** and note that  $F = \mathbb{Q}(\sqrt[3]{2})$ .
 

(a) Show that  $\text{Gal}(E/\mathbb{Q})$  contains an element  $\sigma$  with the property that all elements of  $F$  fixed by  $\sigma$  are rational.

(b) Let  $a \in F$  and suppose  $a^3 \in \mathbb{Q}$ . Show that one of  $a, a\sqrt[3]{2}$  or  $a\sqrt[3]{4}$  is contained in  $\mathbb{Q}$ .

(c) Prove that  $\sqrt[3]{3} \notin E$ .



18. SPRING 2010

1. (a) Up to **similarity**, list all  $4 \times 4$  matrices in  $M_4(\mathbb{C})$  which have **characteristic polynomial**  $\lambda(\lambda - 1)^3$ .  
 (b) For each matrix you gave above, write down its **minimal polynomial**.  
 (c) Let  $A \in M_n(\mathbb{C})$ . Prove that  $A$  is **similar** to a **diagonal matrix** if and only if its **minimal polynomial** has **distinct** roots.
  
2. Let  $V$  be a finite-dimensional **inner product space** over  $\mathbb{C}$  and let  $T$  be a **linear operator** on  $V$ .  
 (a) Define the **adjoint** of  $T$  and define what it means for  $T$  to be **self-adjoint**.  
 Recall that  $T$  is said to be **normal** if it **commutes** with its adjoint.  
 (b) Prove that if  $T$  is normal then  $T$  and its adjoint  $T^*$  have the same **kernel**.  
 (c) Prove that if  $T$  is normal and  $T = T^2$  then  $T$  is self-adjoint.  
 (d) Prove that if  $T$  is normal and **nilpotent**, then  $T = 0$ .
  
3. Let  $S$  and  $T$  be **commuting operators** on a finite-dimensional vector space  $V$  over an **algebraically closed field**  $k$ .  
 (a) Prove that  $S$  and  $T$  have a **common eigenvector**.  
 (Hint: *You may use the fact that any operator on a vector space over  $k$  has at least one eigenvector.*)  
 (b) If  $V$  has a **basis of eigenvectors** of  $S$  and a basis of eigenvectors of  $T$ , show that it has a basis consisting of vectors that are eigenvectors for both  $S$  and  $T$ .  
 (c) What does (b) say about matrices?
  
4. Let  $p$  and  $q$  be **distinct primes** with  $p < q$  and  $q \not\equiv 1 \pmod{p}$ . Let  $G$  be a **group of order**  $pq$ . Prove that  $G$  is **cyclic**.
  
5. (a) Define what it means for a group  $G$  to be **simple**.  
 (b) Prove that if  $|G| = 30$ , then  $G$  is **not simple**.
  
6. Let  $S_4$  be the **symmetric group** on 4 letters. Prove or disprove: every two subgroups of  $S_4$  of order 4 are **conjugate**.
  
7. Let  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ .  
 (a) Compute the **Galois group** of  $K$  over  $\mathbb{Q}$ . Explain fully.  
 (b) List the distinct subfields of  $K$ .  
 (c) Is the **extension**  $K/\mathbb{Q}$  Galois? If so, indicate the **Galois correspondence** between (a) and (b).
  
8. (a) Define what it means for an **algebraic extension**  $k \subseteq K$  of fields to be **normal**.  
 (b) Find an algebraic extension of  $\mathbb{Q}$  which is **not normal**. Explain fully.
  
9. Let  $R$  be a **commutative ring with 1**,  $N$  a **nilpotent ideal** of  $R$ , and  $\pi: R \rightarrow R/N$  the **quotient map**.  
 (a) Prove that if  $\pi(r)$  is a **unit** (invertible element) in  $R/N$ , then  $r$  is a unit in  $R$ .  
 (b) Prove that the induced map from  $\text{GL}_n(R)$  to  $\text{GL}_n(R/N)$  is surjective.  
 (Hint: *Recall that  $\text{GL}_n(R)$  denotes the **group of invertible  $n \times n$  matrices** over  $R$ .*)

10. Let  $k$  be a field.
- (a) Prove that the polynomial ring  $k[t]$  is a principal ideal domain.
  - (b) Suppose that  $I_1 \subseteq I_2 \subseteq \cdots$  is an ascending chain of ideals in a principal ideal domain  $R$ . Prove that there is a number  $N$  such that  $I_N = I_{N+1} = \cdots$ .
  - (c) Prove that every element of a principal ideal domain  $R$  is a product of irreducible elements.
11. Let  $R$  be an integral domain with field of fractions  $F$ .
- (a) Define what it means for an element  $a$  of  $F$  to be *integral* over  $R$ .
  - (b) Define what it means for  $R$  to be *integrally closed*.
  - (c) Show that a unique factorization domain is integrally closed.

1. (a) State the three **Sylow theorems**.  
 (b) Determine, up to **isomorphism**, all **groups** of order 21.
2. Let  $p$  be a prime and  $n$  a positive integer. Prove that any **group** of order  $p^n$  is **solvable**.
3. Prove or disprove each of the following statements.
  - (a) If  $H_1$  and  $H_2$  are **groups** and  $G = H_1 \times H_2$ , then any **subgroup** of  $G$  is of the form  $K_1 \times K_2$ , where  $K_1$  is a **subgroup** of  $H_1$  and  $K_2$  is a **subgroup** of  $H_2$ .
  - (b) If  $G$  is a **group** and  $H$  and  $N$  are **subgroups** of  $G$  with  $H$  **normal** in  $N$  and  $N$  **normal** in  $G$ , then  $H$  is **normal** in  $G$ .
  - (c) If  $G_1$  and  $G_2$  are **groups**,  $N_1 \trianglelefteq G_1$ ,  $N_2 \trianglelefteq G_2$ ,  $N_1 \simeq N_2$ , and  $G_1/N_1 \simeq G_2/N_2$ , then  $G_1 \simeq G_2$ .
4. Prove that for any positive integer  $n$ , if  $G$  is a **nonabelian simple subgroup** of  $S_n$ , then  $G \subseteq A_n$ .
5. Let  $R$  be an **integral domain**, and let  $Q_R$  denote its **field of quotients**. Let  $P$  be a **prime ideal** of  $R$ , and define  $L_P = \{\frac{m}{n} \in Q_R \mid n \notin P\}$ . Prove that  $L_P$  is a **subring** of  $Q_R$ .
6. Let  $R$  be a finite **commutative ring** with **unity**. Prove that every **prime ideal** of  $R$  is **maximal**.
7. (a) Give an example of a **principal ideal domain** that is not a **field**.  
 (b) Give an example of a **unique factorization domain** that is not a **principal ideal domain**.  
 (c) Give an example of an **integral domain** that is not a **unique factorization domain**.
8. Let  $V$  be a **finite-dimensional, real inner product space** with **inner product**  $\langle \cdot, \cdot \rangle: V \times V \rightarrow \mathbb{R}$ . Let  $f: V \rightarrow \mathbb{R}$  be a **linear functional**.
  - (a) Prove that there exists  $w \in V$  such that  $f(v) = \langle v, w \rangle$  for all  $v \in V$ .
  - (b) Prove that  $w \in V$  above is uniquely determined by  $f$ .
9. Find four **non-conjugate**, 6-by-6, complex matrices, each with **characteristic polynomial**  $(t^2-1)(t^4-1)$ .
10. Let  $V$  be a **finite-dimensional vector space** over  $\mathbb{C}$  and let  $f: V \rightarrow V$  be a **linear transformation**.
  - (a) Define the **rank** of  $f$ .
  - (b) Define the **minimal polynomial**  $m(f)$  of  $f$ .
  - (c) Find a **linear transformation**  $f: \mathbb{C}^5 \rightarrow \mathbb{C}^5$  such that  $\text{rank}(f) = 4$  and  $m(f) = t(t-1)^2$ .
11. Let  $V$  be an  **$n$ -dimensional vector space** over  $\mathbb{C}$  and let  $f: V \rightarrow V$  be a **linear transformation**. Prove that there exists a **basis**  $B = \{v_1, \dots, v_n\}$  of  $V$  such that  $f$  is in **upper-triangular form** with respect to  $B$ .
12. Let  $f(x) = x^3 - 2x^2 + 3x - 5$ . Assume that  $f$  has roots  $\alpha$ ,  $\beta$  and  $\gamma$ . Calculate  $\alpha^3 + \beta^3 + \gamma^3$ .
13. (a) Find the **splitting field**  $K$  of  $f(x) = x^3 - 2$  over  $k = \mathbb{Q}$ .  
 (b) Find the **splitting field**  $K$  of  $f(x) = x^2 + 2$  over  $k = \mathbb{R}$ .  
 (c) Find the **splitting field**  $K$  of  $f(x) = x^n - 1$  over  $k = \mathbb{Q}$ .  
 (d) Find the **degree** of each **splitting field** in (a), (b) and (c) and identify the **Galois group**  $G = \text{Gal}(K/k)$  in each case.

14. Let  $k \subseteq K$  be a **finite extension** of **fields**.
- (a) Define what it means for  $k \subseteq K$  to be **separable**.
  - (b) Define what it means for  $k \subseteq K$  to be **normal**.
  - (c) Let  $0 \neq f \in k[t]$  and let  $f'$  be the **formal derivative** of  $f$ . Prove that if  $f$  and  $f'$  have a common factor of degree  $\geq 1$  then  $f$  has a **multiple zero** in its **splitting field** over  $k$ .

20. SPRING 2008

- Let  $E/F$  be a Galois extension of fields of degree 100. Show that there is a unique intermediate field  $M$  of degree 4 over  $F$  and that  $M$  is Galois over  $F$ .
- For a prime number  $p$  let  $\mathbb{F}_{p^n}$  be the field with  $p^n$  elements.
  - List all intermediate fields of the extension  $\mathbb{F}_{p^{12}}/\mathbb{F}_p$ . Draw a diagram illustrating all inclusions between these fields.
  - Determine the number of elements of  $\mathbb{F}_{p^{12}}$  such that  $\mathbb{F}_{p^{12}} = \mathbb{F}_p(\alpha)$ .
- Let  $H$  be a subgroup of a group  $G$  of finite order, and  $(G : H)$  equal the smallest prime that divides the order of  $G$ . Prove that  $H$  is normal.
- Let  $G$  be a group. Suppose that  $m$  and  $n$  are relatively prime integers such that

$$\begin{aligned}x^n y &= y x^n, \\ y^m x &= x y^m\end{aligned}$$

for any  $x, y \in G$ . Prove that  $G$  is abelian.

- Let  $H$  be a normal subgroup of a finite group  $G$  such that  $(G : H)$  is relatively prime to  $p$  where  $p$  is a prime number that divides the order of  $G$ . Prove that  $H$  contains every  $p$ -Sylow subgroup of  $G$ .
- Give an example of ideals  $I$  and  $J$  of a ring  $R$  such that  $IJ \neq I \cap J$ .
  - Let  $A$  be a commutative ring with unity, and let  $\mathfrak{a} \subseteq A$  be an ideal such that every element of  $1 + \mathfrak{a}$  is invertible. Let  $M$  a finitely generated  $A$ -module, and  $M' \subset M$  be any submodule. Then  $M' + \mathfrak{a}M = M$  implies that  $M' = M$ .

- Let  $V$  be the space of polynomials of degree at most 2 over  $\mathbb{C}$ , and let  $T: V \rightarrow V$  be the linear operator

$$T(p(x)) = -p(x) = \frac{d}{dx}(p(x)).$$

- Is  $T$  diagonalizable?
  - Find a Jordan canonical form of  $T$ .
- Let  $k$  be a field, and let  $x_0, x_1, \dots, x_n$  be  $n + 1$  algebraically independent variables over  $k$ . Show that the dimension of the  $k$  vector space  $A_i \subseteq k[x_0, x_1, \dots, x_n]$  of degree  $i$  homogeneous polynomials is equal to  $\binom{n+i}{i}$ .

1. Prove that if  $A$  is a ring,  $M$  is a **Noetherian  $A$ -module**, and  $E$  is a subset of  $M$ , then there exists a finite subset  $F$  **generating** the same submodule as  $E$  does.
2. Find all **finite groups**  $G$  for which the **automorphism group**  $\text{Aut}(G)$  is trivial. (Give a complete justification.)  
(Hint: *First consider conjugations to show that  $G$  must be abelian.*)
3. For any field  $F$ , consider the **linear transformation** on  $M_{nn}(F)$  given by letting  $f(T) = ST - TS$  for  $T \in M_{nn}(F)$ , where  $S$  is an  $n \times n$  matrix. Prove that if  $S$  is **nilpotent** then so is  $f$ .
4. Does the **symmetric group**  $S_n$  (assume  $n \geq 4$ ) have more elements of odd order, or of even order? Justify.
5. Show that the polynomial  $x^4 + 1$  is **reducible** in  $\mathbb{F}_p[x]$  for all primes  $p$  by doing the following exercises.
  - (a) Show that  $x^4 + 1$  is reducible in  $\mathbb{F}_2[x]$ .
  - (b) If  $p$  is an odd prime, show that 8 divides  $p^2 - 1$ .
  - (c) Use (b) to show that
 
$$x^4 + 1 \mid x^8 - 1 \mid x^{p^2-1} - 1 \mid x^{p^2} - x.$$
  - (d) Use (c) to show that  $x^4 + 1$  is reducible in  $\mathbb{F}_p$  for odd primes  $p$ .
6. (a) Show that, for positive integers  $m, n$ ,
 
$$\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$$
 as abelian groups, where  $d = \gcd(m, n)$ .  
 (b) If  $A$  and  $B$  are **abelian groups** of **order** 40 and 300, respectively, what can you say about the order of  $\text{Hom}_{\mathbb{Z}}(A, B)$ ?
7. Let  $R$  be a **commutative ring** and let  $f: M \rightarrow M$  be a  **$R$ -module homomorphism** from a module  $M$  to itself.
  - (a) If  $M$  is a **Noetherian  $R$ -module** and  $f$  is **surjective**, then show that  $f$  must also be **injective**.
  - (b) If  $M$  is an **Artinian  $R$ -module** and  $f$  is **injective**, then show that  $f$  must also be **surjective**.
  - (c) Is (a) still true if  $M$  is not Noetherian?  
(Hint: *Consider the maps  $f^n$ , for  $n \geq 1$ .*)
8. Show that a square matrix over a field is **similar** to its **transpose**.
9. (a) Define **principal ideal domain**.  
 (b) Prove  $\mathbb{Z}$  is a principal ideal domain.  
 (c) Which of the following rings are principal ideal domains?
  - (i)  $\mathbb{Z}[i]$ ;
  - (ii)  $\mathbb{Z}[\sqrt{-5}]$ ;
  - (iii)  $\mathbb{Z}[x]$ ;
  - (iv)  $\mathbb{C}[x]$ .

No reasons are required for part (c).

10. Suppose  $\alpha$ ,  $\beta$ , and  $\gamma$  are the roots of  $t^3 - 2t + 5$ .
- (a) What is  $\alpha\beta + \beta\gamma + \alpha\gamma$ ?
  - (b) What is  $\alpha^2 + \beta^2 + \gamma^2$ ?
11. Let  $G$  be the **Galois group** of  $\mathbb{Q} \subseteq L$ , where  $L$  is the **normal closure** of  $\mathbb{Q}(\sqrt[8]{2})$ .
- (a) What is  $[L : \mathbb{Q}]$ ?
  - (b) Construct  $L$  as a subfield of  $\mathbb{C}$ .
  - (c)  $G$  is the symmetry group of which **regular polygon**?
  - (d) Find **generators** for  $G$ .
12. Let  $R$  be a commutative ring with 1, and let  $\mathfrak{N} = \{x \in R : x^n = 0 \text{ for some } n > 0\}$ , the **nilradical** of  $R$ .
- (a) Prove that  $\mathfrak{N}$  is an ideal of  $R$ .
  - (b) Suppose  $e = e^2$  in  $R/\mathfrak{N}$ . Prove that there exists  $f = f^2$  in  $R$  such that  $\pi(f) = e$ , where  $\pi: R \rightarrow R/\mathfrak{N}$  is the quotient map.

22. FALL 2006

1. How many **conjugacy classes** of matrices  $A$  in  $\text{GL}_6(\mathbb{C})$  are there with the property that  $A^5 = 0$ ? Justify your answer.
2. An element  $\alpha \in \mathbb{C}$  is called an **algebraic integer** if  $m_{\alpha, \mathbb{Q}}(x) \in \mathbb{Z}[x]$  (where  $m_{\alpha, \mathbb{Q}}(x)$  denotes the **minimal polynomial** for  $\alpha$  over  $\mathbb{Q}$ ). Let  $\mathbb{A} \subset \mathbb{C}$  denote the subset of all algebraic integers.
  - (a) Let  $a$  be an algebraic integer with minimal polynomial over  $\mathbb{Q}$  of **degree**  $r$ .
    - (i) Prove that  $\mathbb{Z}[a]$ , the set of all polynomials in  $a$  with integer coefficients, is equal to
 
$$\{c_0 + c_1a + \cdots + c_{r-1}a^{r-1} : c_0, c_1, \dots, c_{r-1} \in \mathbb{Z}\}.$$
    - (ii) Let  $b \in \mathbb{Z}[a]$ , and consider  $L_b: \mathbb{Q}(a) \rightarrow \mathbb{Q}(a)$  given by  $L_b(x) = bx$ . Let  $A$  be the  $r \times r$  **matrix that represents**  $L_b$  relative to the ordered  $\mathbb{Q}$ -basis  $(1, a, \dots, a^{r-1})$  for  $\mathbb{Q}(a)$ . Prove that  $A$  has integer entries. Conclude that the **characteristic polynomial**  $c_A(x)$  for  $A$  is a monic polynomial with integer coefficients and that  $c_A(b) = 0$ .
  - (b) Prove that  $\mathbb{A}$  is a **subring** of the field of algebraic integers of  $\mathbb{C}$ .
  - (c) For  $\alpha \in \mathbb{A}$ , establish necessary and sufficient conditions on  $m_{\alpha, \mathbb{Q}}$  in order that  $\alpha^{-1} \in \mathbb{A}$ .
  - (d) Prove that  $\alpha = \sqrt{2} + \sqrt{5} \in \mathbb{A}$ . Is  $(\sqrt{2} + \sqrt{5})^{-1} \in \mathbb{A}$ ?
3. Let  $n > 1$  be an integer and  $k$  be a positive divisor of  $n$  with  $k < n$ , so  $x^k - 1$  is a divisor of  $x^n - 1$  in  $\mathbb{Z}[x]$ . Let  $q(x) \in \mathbb{Z}[x]$  be such that  $x^n - 1 = (x^k - 1)q(x)$ . Prove that  $\Phi_n(x)$  divides  $q(x)$  in  $\mathbb{Z}[x]$  where  $\Phi_n(x)$  denotes the  $n^{\text{th}}$  **cyclotomic polynomial**.
4. Compute the **Galois group** of the extension  $\mathbb{Q}(2^{1/3}, 2^{1/2})$  of  $\mathbb{Q}$ .
5. Prove that if  $E$  and  $F$  are fields such that  $E$  is a **finite extension** of  $F$ , then  $E$  is an **algebraic extension** of  $F$ .
6. Let  $k$  be a field and let  $V$  be a finite-dimensional vector space over  $k$ . Given a linear transformation  $T: V \rightarrow V$ , prove that there exist  **$T$ -invariant subspaces**  $U$  and  $W$  of  $V$  such that  $V = U \oplus W$ ,  $T|_U$  is a **nilpotent** linear operator on  $U$  and  $T|_W$  is an **invertible** linear operator on  $W$ .
7. Let  $G$  be a finite group of **order**  $n$ .
  - (a) Prove that the number of elements in any **conjugacy class** of  $G$  divides  $n$ .
  - (b) Suppose that  $n = p^m$  for some prime  $p$  and positive integer  $m$ . Prove that the **centre** of  $G$  is nontrivial.
8. Prove that the multiplicative group of a **finite field** is cyclic.
9. Let  $G$  be a **simple group** of order 168. How many elements of order 7 does  $G$  have?



23. SPRING 2006

1. Show that two  $6 \times 6$  nilpotent matrices with the same rank and minimal polynomial must be similar. Find an example of two  $7 \times 7$  nilpotent matrices with the same rank and minimal polynomial that are not similar.
2. Prove that there are no simple groups of order  $2^m \cdot 5$  for any integer  $m \geq 1$ .
3. Let  $p$  be a prime. Choose  $b \in \mathbb{Q}$  not a  $p$ th root in  $\mathbb{Q}$ . Let  $K$  be the splitting field of  $x^p - b$  over  $\mathbb{Q}$ .
  - (a) Prove that  $K$  is generated over  $\mathbb{Q}$  by a  $p$ th root  $\alpha$  of  $b$  and a primitive  $p$ th root of unity  $\zeta$ .
  - (b) Prove that  $[K : \mathbb{Q}] = p(p - 1)$ .
  - (c) Prove that  $G = \text{Gal}(K/\mathbb{Q})$  is isomorphic to the group
 
$$\begin{pmatrix} \mathbb{F}_p^* & \mathbb{F}_p \\ 0 & 1 \end{pmatrix}.$$
  - (d) Let  $\sigma$  be a generator of the group  $\mathbb{F}_p^*$ . Find a presentation of  $G$  in terms of the generators
 
$$x = \begin{pmatrix} \sigma & 0 \\ 0 & 1 \end{pmatrix} \text{ and } y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$
4. If  $G$  is an abelian group of order 56, what are the possible values of  $|\text{Aut}(G)|$ ?
5. Suppose  $A \in M_{n,n}(\mathbb{C})$ .
  - (a) Show that  $A, A^*A$ , and  $AA^*$  all have the same rank.
  - (b) If  $A$  and  $A^*$  commute, and  $p(t)$  and  $q(t)$  are relatively prime polynomials, show that the nullspace of  $p(A)$  and the nullspace of  $q(A)$  are orthogonal.
6. Suppose that  $R$  is a PID and  $a, b \in R$  are nonzero elements for which the ideal  $(a, b)$  equals  $R$ . Prove that  $\text{Hom}_R(R/(a), R/(b)) = 0$ .
7. Find all the ring isomorphisms  $\phi: \mathbb{Z}[t] \rightarrow \mathbb{Z}[t]$ . Prove you are right.
8. Let  $R$  be a commutative ring. Show that a submodule of a free  $R$ -module must be torsion-free, but (by example) need not be free.

24. SPRING 2005

1. (a) List all **abelian groups** (up to **isomorphism**) of **order 200**.  
(b) State the precise relationship between abelian groups of order  $p^n$  and **partitions of  $n$** .
2. (a) Prove that if  $G$  is **group of order  $p^2$** , then  $G$  is **abelian**.  
(b) Exhibit a group  $G$  of **order  $p^3$**  that is **not abelian**.
3. (a) Prove that a  **$n \times n$  matrix over  $\mathbb{C}$**  satisfying  $A^m = I_n$  can be **diagonalized**.  
(b) Is (a) true for any **algebraically closed field of  $k$** ? If not, give a counterexample. If so, give a reason.
4. Let  $k$  be a **field** and let  $V$  be a **finite-dimensional vector space** over  $k$ . Let  $T: V \rightarrow V$  be a **linear transformation**. Prove that there exists a **direct sum decomposition**  $V = U \oplus W$  such that
  - (a)  $T|_U$  is **nilpotent**.
  - (b)  $T|_W$  is **invertible**.
5. Let  $H$  and  $K$  be **subgroups** of a group  $G$ . Prove that the following are equivalent.
  - (a)  $HK = KH$ .
  - (b)  $HK$  is a subgroup of  $G$ .
6. (a) Define what it means for a **finite field extension  $K \subseteq L$**  to be **normal**.  
(b) Find a finite extension  $L$  of  $\mathbb{Q}$  that is not normal.
7. Let  $G = \text{GL}_n(\mathbb{Z}/p\mathbb{Z})$ .
  - (a) Give a formula, in terms of  $n$  and  $p$ , for the **order** of  $G$ .
  - (b) Exhibit a  **$p$ -Sylow subgroup**  $U$  of  $G$ .
  - (c) Why is the **number of  $p$ -Sylow subgroups** of  $G$  not divisible by  $p$ ?

1. (a) Find two matrices  $A$  and  $B$  in  $M_4(\mathbb{C})$  which both have **characteristic polynomial**  $\lambda(\lambda+1)(\lambda-1)^2$  but which are not **similar**.  
 (b) Can you find an example for which  $A$  and  $B$  have the same **minimal polynomial**?  
 (c) Let  $A \in M_n(\mathbb{C})$ . Prove that  $A$  is **similar** to a diagonal matrix if and only if its **minimal polynomial** has distinct roots.
2. Let  $T$  be a **linear operator** on a **finite-dimensional vector space**  $V$  over a field  $k$ . Prove that there exists a **decomposition**  $V = X \oplus Y$  with  $X$  and  $Y$   $T$ -invariant, such that  $T|_X$  is **invertible** and  $T|_Y$  is **nilpotent**.
3. Let  $V$  be a **finite-dimensional inner product space** over  $\mathbb{C}$  and let  $T$  be a **linear operator** on  $V$ .  
 (a) Define the **adjoint** of  $T$  and define what it means for  $T$  to be **self-adjoint** and **normal**.  
 (b) Prove that if  $T$  is **normal** then  $T$  and its **adjoint**  $T^*$  have the same **kernel**.  
 (c) Prove that if  $T$  is **normal** and  $T = T^2$  then  $T$  is **self-adjoint**.  
 (d) Prove that if  $T$  is **normal** and **nilpotent**, then  $T = 0$ .
4. Let  $S$  and  $T$  be operators on a **finite-dimensional vector space**  $V$  over an **algebraically closed field**  $k$ .  
 (a) Show that  $S$  and  $T$  have a common **eigenvector**.  
 (b) If  $V$  has a **basis of eigenvectors** of  $S$  and a basis of eigenvectors of  $T$ , show that it has a basis consisting of vectors that are eigenvectors for both  $S$  and  $T$ .  
 (c) What does (b) say about matrices?
5. (a) Define what it means for a **subgroup**  $H$  of a group  $G$  to be **normal**.  
 (b) Show that if  $H$  has **index 2** in  $G$ , then  $H$  is **normal**.
6. (a) Define what it means for a group  $G$  to be **simple**.  
 (b) Show that if  $|G| = pq$ , where  $p$  and  $q$  are distinct primes, then  $G$  is not simple.
7. Prove that the group of **units** in a field is **cyclic**.
8. What is the **Galois group** of  $x^3 - 3x + 1$  over  $\mathbb{Q}$ ?
9. Let  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ .  
 (a) Compute the **Galois group** of  $K$  over  $\mathbb{Q}$ .  
 (b) List the distinct **subfields** of  $K$ .  
 (c) Indicate the Galois correspondence between (a) and (b).
10. (a) Let  $V$  be a **finite-dimensional vector space** over a **field**  $k$ , and denote by  $R$  the **ring of operators** on  $V$ . Then  $V$  is a **left  $R$ -module**, where  $Tv = T(v)$  for  $T \in R$  and  $v \in V$ . Prove that  $V$  is a **simple  $R$ -module**.

- (b) Prove that if  $M$  is any **simple module** over any **ring**  $R$ , the ring  $\text{Hom}_R(M, M)$  is a **division ring**.
11. Let  $R$  be a **commutative ring** with 1,  $N$  a **nilpotent ideal** of  $R$ , and  $\pi: R \rightarrow R/N$  the **quotient map**.
- (a) Show that if  $\pi(r)$  is a **unit** (invertible element) in  $R/N$ , then  $r$  is a unit in  $R$ .
- (b) Prove that the induced map from  $\text{GL}_n(R)$  to  $\text{GL}_n(R/N)$  is surjective.
12. Let  $k$  be a **field**.
- (a) Show that the **polynomial ring**  $k[t]$  is a **principal ideal domain**.
- (b) Suppose that  $I_1 \subseteq I_2 \subseteq \dots$  is an ascending **chain of ideals** in a **principal ideal domain**  $R$ . Show that there is a number  $N$  such that  $I_N = I_{N+1} = \dots$ .
- (c) Show that every element of  $k[t]$  is a product of **irreducible elements**.

26. SPRING 2004

- Let  $V$  be a **finite-dimensional, complex vector space** with a **Hermitian inner product**. Let  $T: V \rightarrow V$  be a **self-adjoint linear transformation**.
  - Show that every **eigenvalue** of  $T$  is real.
  - Is  $T$  **diagonalizable**? Prove or disprove.
- Prove that there are no **simple groups** of order 80.
- If  $G$  is an **abelian group** of order 175, what are the possible values of  $|\text{Aut}(G)|$ ?
- How many **conjugacy classes of matrices**  $A$  in  $\text{GL}_6(\mathbb{C})$  are there with the property that  $(A - I)^5 = 0$ ? Justify.
- If  $G$  is a group, the **Frattini subgroup**  $\Phi(G)$  is defined to be the intersection of all **maximal proper subgroups** of  $G$ . Prove that, if  $N \trianglelefteq G$ , then  $\Phi(N) \trianglelefteq \Phi(G)$ .
- Suppose  $A \in \text{GL}_4(\mathbb{F}_3)$  is a **nonidentity matrix** satisfying  $A^3 = I$ . What are the possible values for the **rational canonical form** of  $A$ ?
- Let  $G$  be a group, and let  $H \leq G$  be a **subgroup of index 2** in  $G$ . Prove that  $H$  is **normal** in  $G$ .
  - Show by example that the conclusion in part (a) is not true if  $H \subseteq G$  has index three.
- Let  $K \subseteq L$  be a **finite extension of fields**.
  - Define what it means for  $K \subseteq L$  to be **separable**.
  - Define what it means for  $K \subseteq L$  to be **normal**.
  - Give an example where  $K \subseteq L$  is normal but not separable.
  - Give an example where  $K \subseteq L$  is separable but not normal.
- Let  $G = \text{GL}_n(\mathbb{Z}/p\mathbb{Z})$  where  $p$  is a prime number.
  - What is the **order** of  $G$  in terms of  $n$  and  $p$ ?
  - Exhibit a  **$p$ -Sylow subgroup** of  $G$ .
- State the **division algorithm** for  $K[x]$ , where  $K$  is a **field**.
  - Show that  $K[x]$  is a **P.I.D.**.
  - Give an example of an **integral domain** that is not a P.I.D. .
- Let  $p$  and  $q$  be distinct prime numbers. **This exercise is incomplete. Only the previous sentence shows up in the pdf file.**

1. List all **abelian groups of order 400**, up to isomorphism.
2. Exhibit a **3-Sylow subgroup** of  $GL_4(\mathbb{F}_3)$ . Justify your answer with a counting argument.
3. (a) State the **division algorithm** for  $\mathbb{Q}[x]$ .  
 (b) Using (a) prove that any **ideal** of  $\mathbb{Q}[x]$  is a **principal ideal**.
4. Let  $p(x) = x^3 + 3x - 2 \in \mathbb{Q}[x]$  with roots  $\alpha, \beta$ , and  $\gamma$ . Compute
  - (a)  $\alpha\beta + \alpha\gamma + \beta\gamma$
  - (b)  $\alpha + \beta + \gamma$
  - (c)  $\alpha^2 + \beta^2 + \gamma^2$
5. (a) State **Eisenstein's irreducibility criterion**.  
 (b) Using (a) (or otherwise) prove that  $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$  is **irreducible** over  $\mathbb{Q}$ .
6. Let  $R = M_2(K)$  where  $K$ , is any field, and let
 
$$T = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R : c = 0 \text{ and } ad \neq 0 \right\}.$$
 Define  $A \sim B$  in  $R$  if there exist  $X, Y \in T$  such that  $XAY = B$ .
  - (a) Prove that  $\sim$  is an **equivalence relation**.
  - (b) Find a representative for each **equivalence class**.
7. (a) What is the **companion matrix**  $C(f)$  of  $f(x) = x^4 - 4x^3 + 6x^2 - 4x + 1$ ?  
 (b) Find the **Jordan canonical form** of  $C(f)$ .
8. Let  $H$  and  $K$  be subgroups of the group  $G$ . Assume  $H$  is **normal** in  $G$ . Prove  $HK = \{hk \in G \mid h \in H, k \in K\}$  is a **subgroup** of  $G$ .
9. Let  $A$  be a **commutative ring with 1**.
  - (a) Define what it means for a subset  $I \subseteq A$  to be an **ideal** of  $A$ .
  - (b) Let  $N(A) = \{x \in A \mid x^n = 0 \text{ for some } n > 0\}$ . Show that  $N(A)$  is an **ideal** of  $A$ .
10. Let  $p > 0$  be a **prime** number.
  - (a) Prove that any group of order  $p^2$  is **abelian**.
  - (b) Exhibit a **nonabelian group** of order  $p^3$ .
11. Is there a **nonabelian group** of order 33? If not, prove it. If so, exhibit one.

1. List all **groups** of order 6. Prove that your list is complete.
2. Find all **abelian groups** (up to **isomorphism**) of order 360.
3. Let  $\mathbb{F}_q$  be a **finite field** of  $q$  elements. What is the order of the group  $\text{GL}_n(\mathbb{F}_q)$  of  $n \times n$  **invertible matrices** over  $\mathbb{F}_q$ ? Prove your claim.
4. Let  $G$  be a **finite group** and let  $|G|$  be the order of  $G$ .
  - (a) Show that the number of elements in any **conjugacy class** of  $G$  divides  $|G|$ .
  - (b) Let  $G \neq \{1\}$  be a **finite  $p$ -group**. Prove that the **centre** of  $G$  is non-trivial.
5. A complex number  $\alpha \in \mathbb{C}$  is called an **algebraic integer** if there exists an equation
 
$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0$$
 with  $n > 0$  and  $a_i \in \mathbb{Z}$ . Suppose  $\alpha$  and  $\beta$  are algebraic integers.
  - (a) Prove that  $\alpha\beta$  and  $\alpha + \beta$  are **algebraic integers**.
  - (b) Find a polynomial making  $\sqrt{2} + \sqrt{5}$  algebraic.
6. An **automorphism of a field**  $\mathbb{F}$  is a bijection  $f: \mathbb{F} \rightarrow \mathbb{F}$  that preserves the additive and multiplicative structures. Show that the field  $\mathbb{F} = \mathbb{R}$  of real numbers has only one **automorphism**, the identity. How about  $\mathbb{F} = \mathbb{C}$ ?
7. Let  $\mathbb{Q} \subset K$  be the **splitting field** of the polynomial  $x^{p^n} - 1 \in \mathbb{Q}[x]$ . Determine the **Galois group** of  $K$  over  $\mathbb{Q}$ .
8. Let  $\mathbb{F}$  be a **field**. Show that  $M_n(\mathbb{F})$  is a **simple algebra**, i.e., if  $I \subset M_n(\mathbb{F})$  is a **two-sided ideal**, then  $I = (0)$  or  $I = M_n(\mathbb{F})$ .
9. The **centre of an algebra**  $\mathcal{A}$  is defined by  $\mathcal{Z}(\mathcal{A}) = \{a \in \mathcal{A} : ab = ba \text{ for all } b \in \mathcal{A}\}$ . What is the centre of  $M_n(\mathbb{F})$  ( $\mathbb{F}$  is a field)? Prove your statement.
10. Consider the exponential map  $\exp: \mathfrak{sl}(2, \mathbb{C}) \rightarrow \text{SL}(2, \mathbb{C})$ , from  $2 \times 2$  complex matrices with zero **trace** to matrices of **determinant** one. Show that this map is not surjective.
11. Show that the following matrices in  $M_p(\mathbb{Z}/p\mathbb{Z})$ ,  $p$  a prime, are **similar**.

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & 1 & 1 \\ \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}.$$

1. Let  $A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 3 \\ 0 & 0 & 1 & 0 & 4 \\ 0 & 0 & 0 & 1 & 5 \end{pmatrix} \in M_5(\mathbb{C})$ .

Prove that any  $B \in M_5(\mathbb{C})$  which commutes with  $A$  is, in fact, a polynomial in  $A$ .

2. In an integral domain  $A$ :

- An element  $u$  is prime if it is not a unit, and if  $u$  divides  $ab$  implies  $u$  divides  $a$  or  $u$  divides  $b$ .
- An element is irreducible if it is not a unit, and whenever  $u$  can be factored in  $A$  as  $u = xy$ , then  $x$  or  $y$  is a unit.

What is the relation between these concepts?

- (a) prime  $\implies$  irreducible, but not conversely;
- (b) irreducible  $\implies$  prime, but not conversely;
- (c) irreducible  $\iff$  prime; or
- (d) none of the above

Justify your answer.

3. In  $\mathbb{Z}[x]$ , factor  $x^{18} - 1$  into irreducible factors.

4. Recall that in a group  $G$ ,  $x$  is said to be conjugate to  $y$  if  $y = g^{-1}xg$  for some  $g \in G$ . This is an equivalence relation on  $G$ . For the symmetric group  $S_4$ , how many different conjugacy classes are there? For each conjugacy class, determine how many elements are in that class, and exhibit one such element.

5. Let  $H = \langle x \rangle$  be a cyclic group of order 6 and  $K = \langle y \rangle$  a cyclic group of order 5. What is the order of the group  $\text{Aut}(H \times K)$  of all automorphisms of  $H \times K$ ? Briefly explain your reasoning.

6. (a) Let  $K$  be a field, and  $K^* = K \setminus \{0\}$  its multiplicative group. Show that any finite subgroup  $G$  of  $K^*$  is cyclic.

(b) Suppose  $H$  is a finite subgroup of the group  $\mathcal{U}(D)$  of units of an integral domain  $D$ . Is  $H$  necessarily cyclic? Explain.

7. A (not necessarily commutative) ring  $R$  with identity is said to be directly finite if  $ab = 1$  ( $a, b$  in  $R$ ) implies  $ba = 1$ .

(a) Prove that the ring  $\mathcal{L}(V, V)$  of linear operators on a finite-dimensional vector space  $V$  is directly finite.

(b) Show by an example that  $\mathcal{L}(V, V)$  need not be directly finite if  $V$  is not finite-dimensional.

8. How many different isomorphism types of abelian groups are there of order 675? Give one example of each type.

9. (a) Determine the Galois group of  $x^3 - 2$  i.e., of the extension  $\mathbb{Q} \subset \mathbb{F}$  generated by the roots (in  $\mathbb{C}$ ) of the polynomial  $x^3 - 2$ .

(b) Find a subfield  $\mathbb{E}$  with  $\mathbb{Q} \subsetneq \mathbb{E} \subsetneq \mathbb{F}$  where the extension  $\mathbb{Q} \subset \mathbb{E}$  is Galois.



10. Consider the extension  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}, \sqrt{5})$ . What is the degree of the extension, and is it a Galois extension?
11. Let  $\alpha, \beta, \gamma$  be the complex roots of the polynomial  $x^3 + 24x - 1$ . Calculate  $\alpha + \beta + \gamma$  and  $\alpha^3 + \beta^3 + \gamma^3$ .
12. (a) List all the possible rational canonical forms for a  $6 \times 6$  matrix in  $M_6(\mathbb{Q})$  for which the characteristic polynomial is  $(x^2 + 1)(x^2 - 1)^2$ .
- (b) One of the answers to part (a) has  $(x^4 - 1)(x + 1)$  as its minimal polynomial. Which one? And what is its Jordan form (regarding it as a matrix in  $M_6(\mathbb{C})$ )?

- List all **abelian groups** (up to isomorphism) of order 1880.
- Is there a **nonabelian group** of order 28? If not, prove it. If so, exhibit one.
- Exhibit a **nonabelian group** of order  $p^3$  ( $p$  a prime).

4. Express

$$X_1^2 X_2 + X_1^2 X_3 + X_2^2 X_1 + X_2^2 X_3 + X_3^2 X_1 + X_3^2 X_2$$

as a polynomial in  $\sigma_1, \sigma_2$  and  $\sigma_3$  where

$$\sigma_1 = X_1 + X_2 + X_3, \quad \sigma_2 = X_1 X_2 + X_1 X_3 + X_2 X_3, \quad \sigma_3 = X_1 X_2 X_3.$$

- Let  $K = \mathbb{Q}(i, \sqrt[4]{3})$  where  $i^2 = -1$ .
  - Compute the **Galois group** of  $K$  over  $\mathbb{Q}$ .
  - List the distinct **subfields** of  $K$ .
  - Indicate the **Galois correspondence** between (a) and (b).
- Find one representative for each **conjugacy class** of matrix  $A \in M_6(\mathbb{C})$  with
 
$$\det(xI - A) = x^4(x - 1)^2$$
- Find an **irreducible polynomial**  $p(x)$  of degree six in  $\mathbb{Q}[x]$ .
  - Use the polynomial of (a) to construct a **linear transformation**  $T: V \rightarrow V = \mathbb{Q}^6$  with no proper, nontrivial,  **$T$ -invariant subspaces**.
- Let  $G$  be a **group** and consider the group  $\text{Aut}(G)$  of **group automorphisms** of  $G$ . Define  $\phi: G \rightarrow \text{Aut}(G)$  by  $\phi(g)(h) = ghg^{-1}$ .
  - Prove that  $\phi$  is a **group homomorphism**.
  - What is the **kernel** of  $\phi$ ?
  - Prove your answer of (b).
- Find the **rational canonical form** over  $\mathbb{Q}$  of the matrix

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

- Let  $k$  be a **field** and let  $a, b \in k[x]$  with  $b \neq 0$ .
  - Prove there exists  $q, r \in k[x]$  such that  $a = bq + r$  and  $\deg(r) < \deg(b)$ .
  - Prove that  $k[x]$  is a **principal ideal domain**.
  - Compute the order of the finite group  $\text{GL}_3(\mathbb{Z}/4\mathbb{Z})$ .
  - Exhibit a **2-Sylow subgroup** of  $\text{GL}_3(\mathbb{Z}/4\mathbb{Z})$ .
- Let  $R = M_n(\mathbb{C})$ , and let  $I \subseteq R$  be a **two-sided ideal** of  $R$  (in the sense of ring theory). Prove that  $I = (0)$  or else  $I = R$ .

## CONCEPT INDEX

$\mathbb{F}_p[x]$ -module, 2018-F:#4  
 $\mathbb{Z}$ -module, 2019-S:#2  
 $\mathbb{Z}$ -modules, 2016-S:#4  
 $p$ -cycle, 2014-S:#2, 2018-S:#6  
 $p$ -group, 2000-F:#4, 2002-F:#10, 2005-S:#2, 2006-F:#7, 2009-F:#2, 2013-S:#2, 2014-S:#3, 2015-F:#6, 2017-S:#5, 2018-F:#5, 2019-S:#1  
 $p$ -groups, 2016-F:#2  
 $p$ -subgroups, 2010-S:#6  
 $p$ th root of unity, 2006-S:#3

abelian  $p$ -group, 2005-S:#1  
 abelian Galois group, 2014-F:#11  
 abelian group, 2002-F:#1, 2005-S:#2, 2007-F:#6, 2008-S:#4, 2013-F:#4, 2014-F:#8, 2014-S:#1, 2015-F:#6, 2015-S:#11, 2016-F:#1, 2018-F:#5  
 abelian groups of a given order, 1996-F:#1, 1997-F:#8, 2000-F:#2, 2002-F:#1, 2004-S:#3, 2005-S:#1, 2006-S:#4, 2007-F:#6, 2013-F:#4, 2014-F:#1, 2016-F:#1  
 abelian groups with given structure, 2015-F:#2  
 action of Galois, 2016-S:#7  
 additive group of a field, 2015-F:#8  
 adjoint of an operator, 2004-F:#3, 2010-S:#2, 2015-S:#1  
 algebra of matrices over a field, 1996-F:#11, 2000-F:#8, 2011-F:#3  
 algebraic field extension, 2006-F:#5, 2010-S:#8  
 algebraic integer, 2000-F:#5, 2006-F:#2, 2013-F:#7, 2019-S:#7  
 algebraic multiplicity of an eigenvalue, 2013-F:#3, 2018-S:#3  
 algebraic number, 2006-F:#2  
 algebraic unit, 2019-S:#7  
 alternating group, 2010-F:#8, 2018-F:#6  
 Artin ring, 2009-F:#6, 2014-S:#11  
 Artinian module, 2007-F:#7  
 ascending chain condition, 2015-F:#13  
 ascending chain of ideals, 2004-F:#12, 2010-S:#10, 2015-F:#13  
 automorphism, 2014-F:#3  
 automorphism group, 1996-F:#8, 1997-F:#5, 2004-S:#3, 2006-S:#4, 2014-S:#1  
 automorphism of a field, 2000-F:#6  
 automorphisms of  $\mathbb{C}$ , 2000-F:#6, 2014-S:#6  
 automorphisms of  $\mathbb{R}$ , 2000-F:#6, 2014-S:#6

basis, 2013-F:#9, 2014-S:#7, 2015-S:#5, 2016-S:#4  
 basis of eigenvectors, 2004-F:#4  
 binomial coefficient, 2008-S:#8  
 biquadratic extension, 2010-S:#7  
 biquadratic field extension, 1997-F:#10  
 Burnside's theorem, 2004-F:#6, 2006-S:#2, 2010-S:#4

canonical map, 2004-F:#11, 2014-S:#12  
 canonical morphism, 2010-S:#9, 2011-S:#6  
 center of a  $p$ -group, 2000-F:#4, 2006-F:#7  
 center of a group, 2000-F:#4, 2010-F:#4, 2018-F:#5  
 center of an algebra, 2000-F:#9, 2011-F:#3  
 centralizer of a matrix, 1997-F:#1  
 characteristic of a field, 2014-S:#3

characteristic polynomial, 2004-F:#1, 2006-F:#2, 2010-F:#5, 2010-S:#1, 2013-F:#1, 2015-S:#2,  
 2016-S:#5, 2017-F:#8, 2019-S:#3  
 Chinese remainder theorem, 2011-F:#9, 2015-F:#5  
 class equation, 2013-S:#2, 2018-F:#5, 2018-S:#6  
 class formula, 2011-S:#9, 2013-F:#5  
 class representative, 2002-F:#6  
 classification of finite abelian groups, 2013-F:#4  
 codimension of a subspace, 2017-F:#3  
 cokernel of a homomorphism, 2017-S:#3  
 cokernel of a matrix, 2017-S:#3, 2019-S:#2  
 cokernel of a module morphism, 2016-S:#4  
 cokernel of group homomorphism, 2014-F:#8  
 common eigenvectors, 2004-F:#4  
 commutative ring, 2006-S:#8, 2007-F:#7, 2011-S:#5, 2018-S:#1  
 commutative ring with 1, 2002-F:#9, 2004-F:#11, 2007-F:#12, 2008-S:#6, 2009-F:#6, 2010-S:#9,  
 2011-F:#9, 2013-F:#8, 2014-S:#11, 2015-F:#12, 2015-S:#5, 2016-F:#8, 2018-S:#2  
 commuting matrices, 1997-F:#1, 2010-F:#2, 2014-S:#8, 2016-S:#5  
 commuting operators, 2010-S:#3  
 companion matrix, 2002-F:#7  
 complex cube root, 2016-S:#8  
 complex inner product space, 2010-S:#2  
 complex matrices, 2004-F:#1, 2010-F:#2, 2010-S:#1, 2011-F:#4  
 complex matrix, 2006-S:#5, 2009-F:#9, 2013-F:#1, 2014-F:#9, 2015-F:#1, 2016-F:#7, 2018-F:#1,  
 2018-S:#3  
 complex matrix of finite order, 2005-S:#3  
 complex subfield, 2010-F:#9  
 complex vector space, 2004-S:#1, 2009-F:#10, 2016-S:#6, 2017-F:#3  
 compositum extension, 2018-S:#8  
 compositum of Galois extension, 2018-S:#8  
 conjugacy class, 2004-S:#4  
 conjugacy class in a group, 1996-F:#6  
 conjugacy class of a group, 1997-F:#4, 2000-F:#4, 2006-F:#7  
 conjugacy classes, 2011-S:#9, 2018-S:#6  
 conjugacy classes in  $S_n$ , 1997-F:#4, 2011-S:#9  
 conjugacy classes of subgroups, 2013-F:#5  
 conjugate subgroups, 2010-S:#6  
 conjugates of a proper subgroup, 2013-F:#5  
 conjugation, 2010-F:#4  
 conjugation of matrices, 2011-F:#4  
 coprime ideals, 2011-F:#9  
 counting Sylow subgroups, 2010-F:#8  
 cubic polynomial, 2004-F:#8  
 cyclic extension, 2014-F:#3, 2019-S:#5  
 cyclic group, 1997-F:#5  
 cyclic group, 2004-F:#6, 2006-F:#8, 2010-F:#7, 2010-S:#4, 2011-S:#10, 2013-S:#1, 2014-F:#10,  
 2015-F:#3, 2015-S:#10, 2016-S:#4, 2017-F:#1, 2018-F:#5  
 cyclic subgroup, 2017-S:#8  
 cyclotomic extension, 2000-F:#7  
 cyclotomic polynomial, 2000-F:#7, 2006-F:#3, 2011-F:#6, 2016-S:#2  
  
 decomposable module, 2015-S:#4  
 degree inequalities, 2014-F:#12  
 degree of a field extension, 1997-F:#10, 2006-S:#3

degree of a splitting field, 2016-F:#3, 2016-S:#7  
 degrees of field extensions, 2016-S:#8  
 determinant of a matrix, 2013-S:#12  
 diagonal matrix, 2014-F:#4, 2017-F:#6  
 diagonalisable matrix, 2004-F:#1, 2004-S:#1, 2005-S:#3, 2010-F:#2, 2010-S:#1, 2011-F:#1, 2014-F:#9,  
 2015-F:#4, 2017-F:#4, 2017-S:#2  
 diagonalisable operator, 2008-S:#7  
 differentiation of polynomials, 2018-F:#4  
 dihedral group, 2007-F:#11, 2010-F:#3, 2014-F:#10, 2016-S:#3, 2019-S:#8  
 dimension of a space, 2014-S:#8, 2017-F:#3  
 direct sum of vector spaces, 2005-S:#4, 2013-F:#2  
 directly finite ring, 1997-F:#7  
 distinct eigenvalues, 2004-F:#1, 2010-F:#5, 2010-S:#1, 2013-F:#1  
 division ring, 2004-F:#10  
 dual vector space, 2009-F:#8  
  
 eigenbasis, 2010-S:#3, 2011-F:#1  
 eigenspace, 2011-F:#1, 2015-S:#2, 2016-S:#5  
 eigenvalue, 2004-S:#1, 2013-F:#3, 2014-F:#4, 2015-S:#2, 2016-F:#7, 2016-S:#6, 2018-S:#3  
 eigenvalues of integral matrices, 2013-F:#7  
 eigenvector, 2004-F:#4, 2016-S:#6  
 Eisenstein integers, 2011-F:#8  
 Eisenstein numbers, 2011-F:#8  
 Eisenstein's irreducibility criterion, 2002-F:#5, 2011-S:#11  
 elementary divisors, 2015-S:#3  
 elements generating  $S_p$ , 2014-S:#2  
 elements in a finite field of a given degree, 2008-S:#2  
 elements of given order in  $S_n$ , 2007-F:#4  
 elements of given order in a simple group, 2006-F:#9  
 equivalence class, 2002-F:#6  
 equivalence relation, 1997-F:#4, 2002-F:#6  
 Euclidean division algorithm, 1996-F:#10, 2002-F:#3, 2004-S:#10  
 evaluation morphism, 2010-F:#6  
 exponential map, 2000-F:#10, 2011-F:#4  
 extension of finite fields, 2011-S:#12, 2017-F:#9  
  
 factorization, 2004-F:#12  
 factorization of polynomials, 1997-F:#3  
 field, 2015-F:#4  
 field automorphism, 2014-S:#6  
 field extension, 2010-S:#7, 2013-F:#10, 2014-F:#5, 2014-S:#4, 2015-F:#10, 2017-S:#7  
 field extensions without proper subextensions, 2016-S:#1  
 field of fractions, 2010-S:#11, 2011-S:#6, 2015-F:#14  
 fields as vector spaces, 2016-S:#8  
 fields of fractions, 2009-F:#5  
 finite commutative ring, 2009-F:#6  
 finite commutative rings, 2007-F:#6, 2014-S:#11  
 finite extension of a finite field, 2014-F:#3  
 finite field, 2000-F:#3, 2008-S:#2, 2011-S:#12, 2013-F:#6, 2014-F:#3, 2014-S:#3, 2015-S:#9, 2016-S:#1,  
 2017-F:#9, 2018-F:#7, 2018-S:#7, 2019-S:#3  
 finite field extension, 2004-S:#8, 2005-S:#6, 2006-F:#5, 2009-F:#14, 2016-F:#4  
 finite fields, 2019-S:#6  
 finite group, 2016-F:#2, 2018-S:#5, 2019-S:#1

finite group of matrices, 2002-F:#2, 2016-S:#5  
 finite group of units in a field, 1997-F:#6  
 finite groups of a given order, 1996-F:#2, 2005-S:#2, 2008-S:#1  
 finite groups of matrices, 2004-S:#9  
 finite groups with given automorphism group, 2014-S:#1  
 finite groups with trivial automorphism group, 2007-F:#2  
 finite subgroups of unit groups, 2011-S:#10  
 finite vector space, 2018-F:#2  
 finite-dimensional vector space, 2009-F:#8, 2014-S:#9, 2017-F:#3, 2017-S:#4  
 finitely generated module, 2008-S:#6, 2016-F:#10  
 Frattini subgroup, 2004-S:#5  
 free module, 2006-S:#8, 2011-S:#5, 2013-F:#9, 2016-F:#9  
  
 Galois correspondance, 1996-F:#5, 2004-F:#9, 2010-S:#7, 2013-F:#10, 2015-F:#11  
 Galois extension, 1997-F:#10, 2008-S:#1, 2013-F:#10, 2014-F:#5, 2015-S:#12, 2017-S:#7, 2018-S:#8,  
 2019-S:#4  
 Galois group, 1996-F:#5, 1997-F:#9, 2000-F:#7, 2004-F:#8, 2006-F:#4, 2006-S:#3, 2007-F:#11,  
 2009-F:#13, 2010-F:#9, 2010-S:#7, 2011-F:#8, 2011-S:#12, 2013-F:#10, 2014-F:#5, 2014-S:#5,  
 2015-F:#11, 2015-S:#7, 2016-F:#3, 2016-S:#7, 2017-F:#7, 2017-S:#7, 2018-F:#8, 2018-S:#7,  
 2019-S:#4  
 Galois theory of finite fields, 2008-S:#2  
 Gauss' lemma, 2013-S:#5  
 general linear group, 2000-F:#3, 2004-F:#11, 2004-S:#6, 2005-S:#7, 2010-S:#9, 2011-F:#2, 2013-S:#3,  
 2014-S:#3, 2015-F:#4, 2015-S:#11, 2016-S:#5, 2019-S:#6  
 generalized eigenspaces, 2018-F:#1  
 generators of a field extension, 2006-S:#3  
 generators of a group, 2006-S:#3, 2007-F:#11  
 group, 2017-S:#8  
 group acting on a set, 2013-S:#2  
 group automorphism, 2010-F:#4  
 group elements of prime power order, 2016-F:#2  
 group homomorphism, 2017-S:#3  
 group isomorphism, 2014-F:#1  
 group of units in a field, 1997-F:#6, 2004-F:#7  
 groups of a given order, 2000-F:#1, 2002-F:#11, 2004-F:#6, 2009-F:#1, 2010-F:#8, 2010-S:#5,  
 2011-F:#7, 2011-S:#8, 2013-S:#1, 2014-F:#10, 2015-F:#6, 2015-S:#10, 2017-S:#8, 2019-S:#1  
  
 Hasse diagram, 2008-S:#2  
 Hermitian form, 2016-S:#6  
 Hermitian inner product, 2004-S:#1  
 homogeneous polynomial, 2008-S:#8  
 homomorphism of groups, 2014-F:#8  
 homomorphism of modules, 2007-F:#7, 2010-F:#6, 2015-F:#5, 2016-F:#10, 2016-S:#4  
 homomorphism of rings, 2006-S:#6, 2007-F:#6, 2010-F:#1, 2011-S:#6, 2014-S:#10, 2015-F:#12  
  
 ideal, 2002-F:#9, 2007-F:#12, 2011-F:#9, 2014-F:#12  
 idempotent, 2007-F:#12  
 image of a module morphism, 2016-S:#4  
 image of group homomorphism, 2014-F:#8  
 image of vector space morphism, 2015-F:#1  
 index-2 subgroup, 2004-F:#5  
 inner automorphism, 2010-F:#4  
 inner automorphisms, 1996-F:#8  
 inner product space, 2004-F:#3, 2004-S:#1, 2009-F:#8, 2015-S:#1

integral domain, 1997-F:#2, 2004-S:#10, 2009-F:#5, 2010-F:#6, 2010-S:#11, 2011-S:#6, 2015-F:#14,  
 2017-S:#6, 2018-F:#3  
 integral domain which is not a PID, 2004-S:#10  
 integral domain which is not a UFD, 2009-F:#7  
 integral element, 2010-S:#11, 2015-F:#14  
 integrally closed subring, 2010-S:#11, 2015-F:#14  
 intermediate field, 2008-S:#1, 2013-F:#10, 2015-F:#11, 2016-S:#8  
 intersection of ideals, 2008-S:#6  
 invariant subspace, 1996-F:#7, 2006-F:#6, 2013-F:#2, 2015-S:#1  
 invariant vector, 2011-S:#3  
 invertible matrix, 2011-F:#4, 2015-F:#4, 2015-S:#11, 2017-S:#2, 2019-S:#6  
 invertible operator, 2004-F:#2, 2005-S:#4, 2006-F:#6, 2013-F:#2  
 irreducible element, 2004-F:#12, 2017-S:#6, 2019-S:#7  
 irreducible elements of a ring, 2010-S:#10, 2015-F:#13  
 irreducible polynomial, 1997-F:#3, 2014-F:#11, 2014-S:#4, 2015-F:#10, 2015-S:#9, 2018-F:#7  
 irreducible polynomials over finite fields, 2015-S:#9  
 irreducible ring element, 1997-F:#2  
 isomorphic field extensions, 2015-F:#10  
 isomorphic groups, 2010-F:#4, 2015-S:#10  
 isomorphism classes of abelian  $p$ -groups, 2016-F:#1  
 isomorphism of groups, 1997-F:#8, 2000-F:#2, 2005-S:#1, 2009-F:#1, 2014-F:#10, 2016-F:#1  
 isomorphism of rings, 2006-S:#7, 2011-F:#9, 2011-S:#6, 2015-S:#5  
  
 Jordan block, 2016-F:#7  
 Jordan canonical form, 1996-F:#9, 1997-F:#12, 2002-F:#7, 2004-S:#6, 2008-S:#7, 2011-F:#4, 2011-S:#1,  
 2015-S:#2  
 Jordan normal form, 2016-F:#7, 2017-S:#4, 2018-F:#1  
  
 kernel of a group homomorphism, 1996-F:#8  
 kernel of a matrix, 2011-F:#1, 2018-F:#1  
 kernel of a vector space morphism, 2015-F:#1  
 kernel of an operator, 2004-F:#3, 2010-S:#2  
 kernel of group homomorphism, 2014-F:#8  
 Kummer theory, 1996-F:#5, 2006-S:#3, 2019-S:#4  
  
 left module, 2004-F:#10  
 Legendre symbol, 2016-S:#2  
 Lie algebra, 2000-F:#10  
 linear functional, 2009-F:#8  
 linear map, 2011-S:#3, 2014-S:#7  
 linear operator, 2004-F:#3, 2008-S:#7, 2010-S:#2, 2013-F:#2, 2015-F:#1, 2015-S:#1, 2017-S:#4  
 linear transformation, 2005-S:#4, 2006-F:#6, 2007-F:#3, 2009-F:#10, 2015-S:#4  
 local ring, 2016-F:#8  
 localization of a ring, 2009-F:#5  
  
 matrices of finite order, 2005-S:#3, 2015-F:#4  
 matrices over finite fields, 2000-F:#3, 2002-F:#2, 2004-S:#9, 2005-S:#7, 2011-F:#2, 2014-S:#3,  
 2015-S:#11, 2019-S:#6  
 matrices with a given characteristic polynomial, 1997-F:#12  
 matrices with a given minimal polynomial, 2004-S:#4  
 matrices with determinant one, 2000-F:#10  
 matrices with given characteristic polynomial, 1996-F:#6, 2009-F:#9, 2013-F:#7  
 matrices with given minimal polynomial, 2006-F:#1, 2009-F:#10  
 matrices with same minimal polynomial, 2006-S:#1

matrices with trace zero, 2000-F:#10  
 matrices with vanishing trace, 2013-F:#3  
 matrix ring, 2002-F:#6  
 matrix with distinct eigenvalues, 2011-F:#4, 2015-F:#1  
 maximal ideal, 2009-F:#6, 2013-F:#9, 2013-S:#4, 2014-F:#2, 2014-S:#11, 2015-S:#5, 2016-F:#8,  
 2018-S:#2  
 maximal order of a group element, 2018-F:#6  
 maximal subgroup, 2004-S:#5  
 minimal ideal, 2018-S:#1  
 minimal polynomial, 1997-F:#12, 2004-F:#1, 2006-F:#2, 2009-F:#10, 2010-F:#5, 2010-S:#1, 2011-S:#1,  
 2013-F:#1, 2017-F:#6, 2019-S:#3  
 module, 2014-F:#12, 2015-S:#4  
 module of homomorphisms of modules, 2016-F:#10  
 modules over a PID, 2010-F:#6, 2015-S:#4  
 multiplicative group of a field, 2011-S:#10

Nakayama's lemma, 2008-S:#6  
 nilpotent group, 2009-F:#2  
 nilpotent ideal, 2004-F:#11, 2010-S:#9, 2014-S:#12, 2015-F:#12  
 nilpotent matrix, 2006-S:#1, 2007-F:#3, 2011-F:#4, 2014-F:#6, 2017-F:#6  
 nilpotent operator, 2004-F:#3, 2005-S:#4, 2006-F:#6, 2007-F:#3, 2010-S:#2, 2013-F:#2  
 nilpotent ring element, 2007-F:#12, 2017-F:#5  
 nilradical, 2007-F:#12  
 Noetherian module, 2007-F:#7  
 Noetherian ring, 2016-F:#10  
 non-abelian  $p$ -group, 2005-S:#2  
 non-abelian Galois group, 2014-F:#11  
 non-abelian group, 2015-S:#11  
 non-commuting elements, 2016-S:#5  
 non-conjugate matrices, 2009-F:#9  
 non-cubes in finite fields, 2017-F:#9  
 non-cyclic subgroup, 2015-S:#10  
 non-diagonalisable matrix, 2005-S:#3, 2014-F:#9, 2015-F:#4  
 non-free module, 2006-S:#8  
 non-Galois extension, 2010-S:#7  
 non-isomorphic group extensions, 2009-F:#3  
 non-isomorphic groups, 2010-F:#4, 2015-F:#8  
 non-normal extension, 2007-F:#11, 2010-F:#9  
 non-normal field extension, 2004-S:#8, 2005-S:#6, 2010-S:#8, 2016-F:#4  
 non-PID, 2007-F:#9, 2017-S:#1  
 non-principal ideal, 2006-S:#8, 2013-S:#4, 2017-S:#1  
 non-real zeros of real polynomials, 2015-F:#9  
 non-separable field extension, 2004-S:#8, 2016-F:#4  
 non-similar matrices, 2006-S:#1, 2010-F:#5, 2013-F:#1  
 non-simple group, 2010-S:#5, 2015-F:#7  
 nonabelian  $p$ -group, 1996-F:#3  
 nonabelian group, 2002-F:#10, 2010-F:#4  
 nonabelian simple group, 2009-F:#4  
 normal closure, 2006-F:#4, 2007-F:#11  
 normal field extension, 1997-F:#9, 2004-S:#8, 2005-S:#6, 2008-S:#1, 2009-F:#14, 2010-S:#8, 2016-F:#4  
 normal operator, 2004-F:#3, 2010-S:#2  
 normal subgroup, 2002-F:#8, 2004-F:#5, 2004-S:#5, 2008-S:#1, 2009-F:#3, 2011-F:#7, 2011-S:#7,  
 2015-S:#10, 2017-S:#8, 2018-S:#5



normal Sylow subgroup, 2011-F:#7  
 normalizer of a subgroup, 2013-F:#5, 2018-S:#6  
 nullspace, 2006-S:#5  
 number field, 1997-F:#9, 2002-F:#4, 2004-F:#8, 2010-F:#9, 2010-S:#8, 2013-F:#10, 2014-F:#11,  
 2015-F:#11, 2015-S:#12, 2016-S:#7, 2017-F:#7, 2017-S:#7, 2018-F:#8  
 number fields, 2019-S:#5  
 number of Sylow subgroups, 2005-S:#7  
  
 operators with common eigenvectors, 2010-S:#3  
 order of a finite matrix group, 2000-F:#3, 2004-S:#9, 2005-S:#7, 2011-F:#2, 2013-F:#6  
 order of a group, 2017-S:#8  
 order of a group element, 2016-F:#1, 2016-S:#5, 2018-F:#6  
 orders of conjugacy classes in finite groups, 1997-F:#4, 2000-F:#4, 2006-F:#7  
 orders of finite matrix groups, 1996-F:#10  
 orthogonal complement, 2015-S:#1  
 orthogonal matrix, 2017-F:#6  
 orthogonal projection, 2011-F:#1  
 orthogonal subspaces, 2006-S:#5  
 orthogonal transformation, 2017-F:#4  
 orthogonality of eigenvectors, 2016-S:#6  
 orthonormal basis, 2011-F:#1  
  
 partitions of  $n$ , 2005-S:#1  
 perfect field, 2018-F:#7  
 permutation representation, 2013-S:#2  
 PID, 2017-S:#1  
 PID which is not a field, 2009-F:#7  
 polynomial ring, 1996-F:#10, 2002-F:#3, 2004-F:#12, 2006-S:#7, 2010-S:#10, 2013-S:#5, 2015-F:#13  
 polynomials irreducible in an extension, 2014-S:#4  
 polynomials irreducible over  $\mathbb{Q}$ , 1996-F:#7, 2002-F:#5  
 polynomials with big Galois group, 2014-S:#5  
 polynomials with multiple zeros, 2009-F:#14  
 positive characteristic, 2017-S:#2  
 positive-definite form, 2016-S:#6, 2018-S:#4  
 possible automorphism groups, 2004-S:#3  
 power series ring, 2013-F:#8  
 presentation of a group, 2006-S:#3  
 primary decomposition, 2018-F:#4  
 prime field, 2011-S:#12  
 prime ideal, 2009-F:#6, 2014-F:#2, 2014-S:#11, 2017-S:#6, 2018-S:#2  
 prime ring element, 1997-F:#2  
 prime vs. irreducible, 1997-F:#2  
 prime-index subgroup, 2004-F:#5, 2004-S:#7, 2008-S:#3, 2018-S:#5  
 primes in  $\mathbb{Z}[i]$ , 2007-F:#5  
 primitive cube root of unity, 2011-F:#8  
 primitive field extension, 2016-S:#1  
 primitive polynomial, 2013-S:#5  
 primitive root of unity, 2006-S:#3, 2011-F:#5, 2016-S:#2  
 principal ideal, 2013-S:#4, 2017-S:#6  
 principal ideal domain, 1996-F:#10, 2002-F:#3, 2004-F:#12, 2004-S:#10, 2006-S:#6, 2007-F:#9,  
 2009-F:#7, 2010-S:#10, 2014-F:#2, 2015-F:#13, 2015-S:#4, 2016-F:#9  
 product of cyclic groups, 1997-F:#5, 2014-F:#8  
 product of groups, 2009-F:#3, 2015-F:#8

product of ideals, 2008-S:#6  
 product set of subgroups, 2005-S:#5  
 projective module, 2016-F:#9  
 proper ideal, 2013-F:#8, 2018-S:#1  
 pseudo-reflection, 2016-S:#5  
  
 quadratic extension, 2019-S:#4  
 quotient ring, 2004-F:#11, 2010-S:#9, 2015-F:#12, 2017-S:#4  
 quotients of solvable groups, 2011-S:#7  
  
 rank of a linear transformation, 2009-F:#10  
 rank of a matrix, 2006-S:#5, 2018-S:#3  
 ratios of cyclotomic polynomials, 2006-F:#3, 2011-F:#6  
 real cube root, 2016-S:#8  
 real eigenvalues of complex matrices, 2016-S:#6  
 real eigenvalues of Hermitian operators, 2004-S:#1  
 real field, 2015-F:#9  
 real matrix, 2014-F:#4, 2017-F:#8, 2018-S:#4  
 real matrix without a real square root, 2014-F:#4  
 real subfield, 2010-F:#9  
 real vector space, 2017-F:#4  
 reduced row-echelon form of a matrix, 2016-F:#6  
 reducible module, 2015-S:#4  
 reducible polynomials over finite fields, 2007-F:#5  
 relatively prime ring elements, 2006-S:#6, 2015-F:#5  
 ring, 2017-S:#4  
 ring of algebraic integers, 2000-F:#5, 2006-F:#2  
 ring of complex matrices, 2011-S:#2  
 ring of Laurent polynomials, 2014-S:#10  
 ring of linear maps, 1997-F:#7, 2014-S:#9  
 ring of operators, 2004-F:#10  
 root of unity, 2011-F:#5, 2011-S:#10, 2016-S:#2  
 row-echelon form of a matrix, 2016-F:#6  
  
 Schur's lemma, 2004-F:#10  
 self-adjoint operator, 2004-S:#1, 2010-S:#2, 2016-S:#6  
 semi-direct product, 2015-S:#10  
 semidirect product, 2006-S:#3  
 separable field extension, 2004-S:#8, 2009-F:#14, 2016-F:#4  
 separable polynomial, 2018-F:#7  
 similar matrices, 1996-F:#6, 2000-F:#11, 2004-F:#1, 2004-S:#4, 2006-F:#1, 2006-S:#1, 2007-F:#8,  
 2010-F:#5, 2010-S:#1, 2013-F:#1, 2015-S:#3, 2019-S:#3  
 simple algebra, 1996-F:#11, 2000-F:#8, 2011-S:#2  
 simple extension, 2017-S:#7  
 simple group, 2004-F:#6, 2010-F:#8, 2010-S:#5, 2015-F:#7, 2017-S:#5, 2019-S:#1  
 simple groups of a given order, 2004-S:#2, 2006-F:#9, 2006-S:#2  
 simple module, 2004-F:#10  
 simple subgroups of  $S_n$ , 2009-F:#4  
 simple transformation, 1996-F:#7  
 size of a conjugacy class, 2011-S:#9  
 Smith normal form, 2017-S:#3  
 solvable group, 2009-F:#2, 2011-S:#7, 2013-S:#3  
 special linear group, 2000-F:#10, 2013-F:#6

splitting field, 1997-F:#9, 2000-F:#7, 2006-S:#3, 2009-F:#14, 2010-F:#9, 2011-F:#8, 2013-F:#10,  
 2014-F:#11, 2015-F:#11, 2015-S:#7, 2016-F:#3, 2016-S:#7, 2017-F:#7  
 square matrix, 2005-S:#3, 2007-F:#8  
 subextension, 2016-S:#1  
 subfield, 1996-F:#5, 2007-F:#11, 2015-F:#9, 2016-S:#8  
 subgroup, 2005-S:#5, 2009-F:#3, 2013-F:#5  
 subgroup lattice, 2019-S:#8  
 subgroup of Galois group, 2013-F:#10  
 subgroup of index 2, 2004-S:#7  
 subgroup of index coprime to  $p$ , 2008-S:#5  
 subgroups of solvable groups, 2011-S:#7  
 submodule, 2006-S:#8, 2007-F:#1, 2008-S:#6, 2011-S:#5  
 submodule of a Noetherian module, 2007-F:#1  
 subring, 2006-F:#2, 2009-F:#5  
 subspace, 2017-F:#3  
 subspace of invariant vectors, 2016-S:#5  
 sum of ideals, 2014-F:#12  
 surjective homomorphism, 2015-F:#12  
 Sylow subgroup, 1996-F:#10, 2002-F:#2, 2004-S:#9, 2005-S:#7, 2008-S:#1, 2010-F:#8, 2011-F:#7,  
 2014-F:#7, 2015-S:#11, 2016-S:#3, 2017-F:#2, 2019-S:#6  
 Sylow subgroups of finite matrix groups, 1996-F:#10, 2002-F:#2, 2004-S:#9, 2005-S:#7, 2013-F:#6,  
 2014-S:#3, 2015-S:#11  
 Sylow theorem, 2009-F:#1  
 Sylow theorems, 2010-S:#6, 2013-S:#2, 2014-F:#7  
 Sylow theory, 2006-F:#9, 2008-S:#5  
 symmetric bilinear form, 2018-S:#4  
 symmetric functions of roots, 1996-F:#4, 1997-F:#11, 2002-F:#4, 2007-F:#10, 2009-F:#12, 2016-F:#5  
 symmetric group, 1997-F:#4, 2007-F:#4, 2010-S:#6, 2014-S:#2, 2016-S:#3, 2017-F:#2, 2018-F:#6,  
 2018-S:#6  
 symmetric matrix, 2014-S:#8  
  
 tensor product of modules, 2010-F:#7, 2014-F:#12  
 torsion of a module, 2006-S:#8  
 torsion-free module, 2006-S:#8, 2010-F:#6, 2011-S:#5  
 trace of a matrix, 2013-F:#3, 2013-S:#12, 2018-S:#4  
 transpose of a matrix, 2007-F:#8, 2018-S:#4  
 transposition, 2014-S:#2  
 two-sided ideal, 1996-F:#11, 2000-F:#8, 2011-S:#2  
  
 UFD which is not a PID, 2009-F:#7  
 unipotent matrix, 2014-F:#6, 2019-S:#6  
 unipotent ring element, 2017-F:#5  
 unique factorization, 1997-F:#3, 2010-S:#10, 2019-S:#7  
 unique factorization domain, 2009-F:#7, 2010-S:#11, 2015-F:#5, 2015-S:#4, 2018-F:#3  
 unit algebraic integers, 2006-F:#2  
 unit groups of rings of a given order, 2011-S:#4  
 unitary matrices, 2015-S:#11  
 unitary matrix, 2011-F:#1  
 unitary subgroup, 2015-S:#8, 2019-S:#6  
 units of a field, 2017-F:#9  
 units of a finite field, 2006-F:#8, 2015-F:#3  
 units of a ring, 1997-F:#2, 2004-F:#11, 2008-S:#6, 2010-S:#9, 2013-F:#8, 2014-S:#10, 2015-F:#3,  
 2016-F:#8, 2017-F:#1, 2018-S:#2

univariate polynomials, 2018-F:#4  
upper triangular matrix, 2013-S:#3, 2014-S:#7, 2015-S:#5, 2017-F:#6, 2019-S:#6  
  
vector space decomposition, 2004-F:#2, 2013-F:#2  
vector space of homogeneous polynomials, 2008-S:#8  
vector space of matrices, 1997-F:#1, 2006-S:#5, 2007-F:#3, 2015-F:#1, 2018-S:#4  
vector space of matrix, 2014-S:#8  
vector space of polynomials, 2008-S:#7, 2018-F:#4  
vector space over an algebraically closed field, 2004-F:#4, 2010-S:#3, 2014-S:#7  
vector spaces over  $\mathbb{Q}$ , 2011-S:#3  
vector subspace, 2011-F:#1, 2014-S:#8, 2017-F:#8  
  
zero divisors, 2014-S:#9  
zeros of a polynomial, 2009-F:#12, 2015-F:#10  
Zorn's lemma, 2013-F:#9