

BASIC COMPREHENSIVE EXAM IN ALGEBRA
SYLLABUS
REVISED JULY 2026

The textbook for Math 526 and Math 581 is *Abstract Algebra*, 3rd Ed, by D. Dummit and R. Foote. The exam covers Chapters 1, 2, 3 (omit 3.4), 4 (omit 4.6), 7, 8, 9 (omit 9.6), 10 (omit 10.4, 10.5), 12 (omit 12.3), 13 (omit 13.3, 13.6), 14.1, 14.2.

Here is a list of typical homework problems for Math 526 and 581. This is **not** a list of potential exam questions.

- (1) Let G be a group and let $x, g \in G$. Prove that $|x| = |g^{-1}xg|$ and deduce that $|ab| = |ba|$ for all $a, b \in G$.
- (2) Let H be a nonempty finite subset of a group G . Show that H is a subgroup if and only if $ab \in H$ for every $a, b \in H$.
- (3) Let G be a group such that $(ab)^i = a^i b^i$ for three consecutive integers i and all $a, b \in G$. Show that G is Abelian.
- (4) Let G be a finite group and let $x \in G$ be an element of order n . Prove that if n is odd, then $x = (x^2)^k$ for some integer $k \geq 1$.
- (5) Let $Q_8 = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle \subset GL(2; \mathbb{C})$, where $i^2 = -1$. Show that $|Q_8| = 8 = |D_4|$, but $Q_8 \not\cong D_4$. (Q_8 is called the **quaternion group**)
- (6) Prove that if σ is the m -cycle $(a_1 a_2 \dots a_m)$, then for all $i \in \{1, 2, \dots, m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k+i$ is replaced by its least positive residue modulo m . Deduce that $|\sigma| = m$.
- (7) Let σ be the m -cycle $(12 \dots m)$. Show that σ^i is also an m -cycle if and only if i is relatively prime to m .
- (8) Let G be a finite group of even order. Prove that G contains an element $a \neq e$ such that $a^2 = e$.
- (9) Let G, H be two groups and suppose that $\varphi : G \rightarrow H$ is a group isomorphism. Show that $|\varphi(x)| = |x|$ for every $x \in G$. Explain how this shows that any two isomorphic groups have the same number of elements of order $n \in \mathbb{Z}^+$.
- (10) Is (9) true (i.e., $|\varphi(x)| = |x|$ for every $x \in G$) if φ is only assumed to be a homomorphism? Prove it is true or give a counterexample.
- (11) Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is Abelian.
- (12) Prove that if $n \neq m$, then S_n and S_m are not isomorphic.
- (13) Let $G = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \subset GL(2; \mathbb{R})$. Show that $G \simeq D_4$.
- (14) Let G be a group and let $x, y \in G$ with $|x| = n$ and $|y| = m$. Suppose that x and y commute, i.e. $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n .
- (15) Give an example of commuting elements x, y in a group G such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.
- (16) Let G be an Abelian group. Prove that $\{g \in G \mid |g| < \infty\}$ is a subgroup of G (called the *torsion subgroup* of G). Give an explicit example where this set is not a subgroup when G is non-abelian.
- (17) Prove that $\mathbb{Q} \times \mathbb{Q}$ is not a cyclic group.
- (18) Let $H = \{\sigma \in S_n \mid \sigma(n) = n\}$. Show that $H \leq S_n$ and $H \cong S_{n-1}$.

- (19) Let G be an Abelian group of order pq , where $\gcd(p, q) = 1$. Assume that there exists $a, b \in G$ such that $|a| = p$ and $|b| = q$. Show that G is cyclic.
- (20) Let H and K be subgroups of a group G . Show that HK is a subgroup of G if and only if $HK = KH$.
- (21) Prove that if H and K are finite subgroups of a group G whose orders are relatively prime, then $H \cap K = \{e\}$.
- (22) Let G be an abelian group and let n be an integer. Show that the set $H = \{g \in G \mid g^n = e\}$ is a subgroup of G . Give an example to show that H may fail to be a subgroup if G is not abelian.
- (23) Let G be a finite group of order n . Let $a \in G$ and assume that $a^k = e$ for some $k < n$. Is it true that k must divide n ? Explain by either proving this or giving a counterexample.
- (24) Prove that a group that has only a finite number of subgroups is a finite group.
- (25) Prove that the subgroup generated by any two distinct elements of order 2 in S_3 is all of S_3 .
- (26) Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$ if and only if $x^{-1}y^{-1}xy \in N$. [The element $x^{-1}y^{-1}xy$ is called the *commutator* of x and y and it is denoted by $[x, y]$.]
- (27) Let G be a group. Prove that $N = \langle x^{-1}y^{-1}xy \mid x, y \in G \rangle$ is a normal subgroup of G and G/N is abelian.
- (28) Let G be a group such that $G/Z(G)$ is cyclic, where $Z(G) = \{g \in G : gx = xg \ \forall x \in G\}$ is the center of G . Show that G is abelian.
- (29) Let G be a group with order pq , where p, q are primes (not necessarily distinct). Prove that either G is Abelian or $Z(G) = 1$.
- (30) Let p be a prime number. Show that every group of order p^2 is Abelian.
- (31) Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. Prove that if $|H|$ and $[G : N]$ are relatively prime then $H \leq N$.
- (32) Prove that if N is a normal subgroup of a finite group G and $\gcd(|N|, [G : N]) = 1$ then N is the unique subgroup of G of order $|N|$.
- (33) Let G be a group and let a, b be elements of finite order m, n , respectively. If $ab = ba$ and $\langle a \rangle \cap \langle b \rangle = \{e\}$, show that the order of ab is $\text{lcm}(m, n)$.
- (34) Let p be a prime number. Let G be a group of order p^n and let H be a normal subgroup of G with $H \neq \{e\}$. Show that $H \cap Z(G) \neq \{e\}$.
- (35) Prove that if G is a finite abelian group and p is a prime number such that p divides $|G|$, then G has a subgroup of order p . (Hint: Try induction on the order of G . Notice that if H is a proper nontrivial subgroup of G , then H and G/H are groups of smaller order than G .)
- (36) Let p be a prime and let G be a group of order $p^a m$, where p does not divide m . Assume P is a subgroup of G of order p^a and N is a normal subgroup of G of order $p^b n$, where p does not divide n . Prove that $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$.
- (37) Describe the orbit and the stabilizer of a single vertex of the square in the dihedral group D_4 viewed as acting on the square.
- (38) Let H be a subgroup of a group G with finite index. Show that there exists a normal subgroup N of G of finite index contained in H .
- (39) Let G be a group acting transitively on a finite set S with $|S| > 1$. Show that there exists a $g \in G$ such that $gx \neq x$ for every $x \in S$ (i.e., g has no fixed point).
- (40) Let G be a group of order 105. Prove that G has a normal 5-Sylow subgroup and a normal 7-Sylow subgroup.
- (41) Let G be a group of order 312. Prove that G contains a nontrivial normal subgroup.
- (42) Let G be a group of order 231. Prove that $Z(G)$ contains an 11-Sylow subgroup of G and that a 7-Sylow subgroup is normal in G .
- (43) Let G be a group of order 351. Prove that G has a normal Sylow p -subgroup for some prime p dividing 351.

- (44) Let G be a finite group.
- (a) Prove that elements in the same conjugacy class have conjugate centralizers.
 - (b) If $c_1, \dots, c_r$ are the orders of the centralizers of elements from the distinct conjugacy classes prove that

$$\frac{1}{c_1} + \dots + \frac{1}{c_r} = 1.$$

- (45) Let H be a proper subgroup of a finite group G . Show that G is not the union of all the conjugates of H .
- (46) Let R be a ring which is finite. Show that R is an integral domain if and only if R is a field.
- (47) Let R be a ring and $S = M_3(R)$.
- (a) Show that there is a one-to-one correspondence between the set of R -ideals I and the set of S -ideals J given by $I \mapsto J = \{(a_{ij}) \mid a_{ij} \in I\}$.
 - (b) Show that if R is a division ring, then 0 and S are the only S -ideals.
- (48) Let R be a commutative ring with identity. An element $x \in R$ is called *nilpotent* if $x^n = 0$ for some $n \in \mathbb{Z}^+$. Prove that the set of nilpotent elements, called the *nilradical* is an ideal in R . This set is denoted by $\mathcal{N}(R)$.
- (49) Let R be a commutative ring with identity and let I be an R -ideal. Define

$$\text{rad}(I) = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+\},$$

the *radical* of I . Prove that $\text{rad}(I)$ is an ideal containing I and that $(\text{rad}(I))/I$ is the nilradical of the quotient ring R/I , i.e. $(\text{rad}(I))/I = \mathcal{N}(R/I)$.

- (50) Let R be a ring with identity and $I_1, \dots, I_n$ be R -ideals. Show that $R = I_1 + \dots + I_n$ with $I_j \cap \sum_{i \neq j} I_i = 0$ for every j if and only if $1 = e_1 + \dots + e_n$ with $I_i = Re_i$, $e_i \in Z(R)$, $e_i^2 = e_i$, and $e_i e_j = 0$ for $i \neq j$. [$Z(R) = \{a \in R \mid ab = ba \text{ for all } b \in R\}$.]
- (51) Let R be a commutative ring with identity and let $I_1, \dots, I_n$ be R -ideals with $I_i + I_j = R$ whenever $i \neq j$. Show that $I_1 \cap \dots \cap I_n = I_1 \cdot \dots \cdot I_n$.
- (52) Let $R = \mathbb{Z}[\sqrt{d}]$, where d is not 1 and is not divisible by the square of a prime. Define a function N , called the *norm*, from R into the nonnegative integers by $N(a + b\sqrt{d}) = |a^2 - db^2|$. Verify the following four properties:
- (a) $N(x) = 0$ if and only if $x = 0$;
 - (b) $N(xy) = N(x)N(y)$ for all $x, y \in R$.
 - (c) x is a unit in R if and only if $N(x) = 1$;
 - (d) If $N(x)$ is prime, then x is irreducible in R .
- (53) Prove that $\mathbb{Z}[\sqrt{-3}]$ is not a PID by finding an element of this ring that is irreducible but not prime.
- (54) Show that 21 does not factor uniquely in $\mathbb{Z}[\sqrt{-5}]$ as a product of irreducibles.
- (55) Factor the following or prove they are irreducible.
- (a) $X^2 + X + 1$ in $\mathbb{Z}_2[X]$.
 - (b) $X^3 + X + 1$ in $\mathbb{Z}_3[X]$.
 - (c) $X^4 + 1$ in $\mathbb{Z}_5[X]$.
 - (d) $X^p - X$ in $\mathbb{Z}_p[X]$, where p is prime.
 - (e) $X^6 + 30X^5 - 15X^3 + 6X - 120$ in $\mathbb{Z}[X]$.
 - (f) $X^4 + 4X^3 + 6X^2 + 2X + 1$ in $\mathbb{Q}[X]$.
- (56) Prove that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, and find an irreducible polynomial with coefficients in $\mathbb{Q}$ that has $\sqrt{2} + \sqrt{3}$ as a root. Be sure to verify that your polynomial is irreducible.
- (57) Find the specified degrees and justify your answer: $[\mathbb{Q}(2 + \sqrt{3}) : \mathbb{Q}]$. and $[\mathbb{Q}(1 + 2^{1/3} + 4^{1/3}) : \mathbb{Q}]$.
- (58) Let K/F be a field extension, and let $\alpha \in K$. Show that if $[F(\alpha) : F]$ is odd, then $F(\alpha) = F(\alpha^2)$.

- (59) Prove that if the degree of the field extension K/F is prime, then for every subfield E of K for which F is a subfield of E , either $K = E$ or $E = F$.
- (60) Prove that if F is a finite field of characteristic $p > 0$, then the number of elements in F is p^n for some $n > 0$.
- (61) Show that if E/F and K/E are algebraic extensions, then so is K/F .
- (62) For an extension K/F and $\alpha, \beta \in K$ algebraic over F :
- (a) Prove $[F(\alpha, \beta) : F] \leq [F(\alpha) : F][F(\beta) : F]$.
 - (b) Give an example to show that the inequality in (a) can be strict.
- (63) Find the minimal polynomial of $1 + i$ over $\mathbb{Q}$.
- (64) Show that if K/F is an algebraic field extension and R is a subring of K such that F is a subring of R , then R is a field.
- (65) Let $f(X) = X^2 + X - 1 \in \mathbb{Z}_3[X]$. Show that f is irreducible and use f to construct a field with 9 elements. Write down the multiplication table for this field and verify that the nonzero elements of the field form a cyclic group with respect to multiplication.
- (66) Let R be a commutative ring, let I be an ideal of R and let M be an R -module. Prove that $IM = \{\sum_{i=1}^k r_i m_i \mid k > 0, r_i \in R, m_i \in M\}$ is an R -submodule of M .
- (67) Let M be an R -module, where M is a commutative ring. Show that M is a cyclic R -module if and only if $M \cong R/I$ for some ideal I of R .
- (68) Let I be an ideal of the commutative ring R , and let $\{M_\alpha\}$ be a collection of R -modules. For $N = \bigoplus_\alpha M_\alpha$, show that $\bigoplus_\alpha M_\alpha / IM_\alpha$ is isomorphic to N/IN as R/I -modules.
- (69) Let $F_1 = \bigoplus_{i=1}^n R$ and $F_2 = \bigoplus_{i=1}^m R$ be free R -modules, where R is a commutative ring. Show that $F_1 \cong F_2$ if and only if $n = m$. Hint: Use previous problem and some linear algebra.
- (70) Let $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ denote the linear transformation that is the projection onto the line $y = 2x$. List all $F[X]$ -submodules of $\mathbb{R}^2$ (where the $F[X]$ -module structure here is that determined by T).
- (71) Prove that the constant term of the characteristic polynomial of the $n \times n$ matrix A is $(-1)^n \det(A)$.
- (72) Prove that the product of eigenvalues of the $n \times n$ matrix A is $\det(A)$.
- (73) Prove that the sum of eigenvalues of the $n \times n$ matrix A is the trace of A .
- (74) Show that the $F[X]$ -module V_T determined by a linear transformation $T : V \rightarrow V$ is cyclic if and only if the characteristic polynomial of T is the minimal polynomial of T .
- (75) Prove that similar linear transformations of a finite dimensional vector space V have the same minimal polynomials and the same characteristic polynomials. (Hint: This is easy if you use results from class.)
- (76) Find all possible rational canonical forms of 4×4 matrices A over $\mathbb{R}$ satisfying $A^3 = I$.
- (77) Let K be an extension of F of degree n .
- (a) If $\alpha \in K$ define a map $T_\alpha : K \rightarrow K$ by $T_\alpha(x) = \alpha x$. Prove that T_α is a linear transformation of K as an F -vector space.
 - (b) Fix a basis $B = \{\alpha_1, \dots, \alpha_n\}$ for K over F , and let $[T_\alpha]_B$ be the matrix for T_α in the basis B . Prove that the map $\phi : K \rightarrow M_n(F)$ defined by $\phi(\alpha) = [T_\alpha]_B$ is an injective ring homomorphism, so K is isomorphic to a subfield of $M_n(F)$.
 - (c) Show that α is a root of the characteristic polynomial of the matrix $[T_\alpha]_B$. (Hint: explain why α is an eigenvalue of the linear transformation T_α)
- (78) Let $\alpha = 1 + \sqrt[3]{2} + \sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$. Using the basis $B = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ for $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$, find the matrix $[T_\alpha]_B$ from the previous problem. Now find the characteristic polynomial of this matrix. This is a monic polynomial having α as a root, according to the previous problem.
- (79) Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + x^2 + 1$.
- (80) Find all the irreducible polynomials of degrees 1, 2, and 4 over $\mathbb{F}_2$ and prove that their product is $x^{16} - x$.

- (81) Prove that d divides n if and only if $x^d - 1$ divides $x^n - 1$. [Note that if $n = qd + r$ then $x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1)$. You may also assume that these are polynomials over $\mathbb{C}$.]
- (82) Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 - 2$.
- (83) Let K_1 and K_2 be finite extension of F contained in the field K and assume that both are splitting fields over F .
- (a) Prove that their composite K_1K_2 is a splitting field over F .
 - (b) Prove that $K_1 \cap K_2$ is a splitting field over F .
- (84) Let K/F be a field extension.
- (a) Show that if a field K is generated over F by the elements $\alpha_1, \dots, \alpha_n$, then an automorphism σ of K fixing F is uniquely determined by $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$. In particular, show that an automorphism fixes K if and only if it fixes a set of generators for K .
 - (b) Let $G \leq \text{Gal}(K/F)$ be a subgroup of the Galois group of the extension K/F and suppose $\sigma_1, \dots, \sigma_k$ are the generators of G . Show that the subfield E/F is fixed by G if and only if it is fixed by the generators $\sigma_1, \dots, \sigma_k$.
- (85) Show that $\mathbb{Q}(\sqrt{2})$ is not isomorphic to $\mathbb{Q}(\sqrt{3})$.
- (86) Determine the minimal polynomial over $\mathbb{Q}$ of the element $\sqrt{2} + \sqrt{5}$.
- (87) Determine the Galois group of $(x^2 - 2)(x^2 - 3)(x^2 - 5)$. Determine all the subfields of the splitting field of this polynomial.
- (88) Suppose K is a Galois extension of F of degree p^n for some prime p and some $n > 1$. Prove that there are Galois extensions of F contained in K of degrees p and p^{n-1} .
- (89) Suppose M and N are R -modules and $\phi : M \rightarrow N$ is an R -module homomorphism. Prove that the kernel of ϕ is a submodule of M and the image of ϕ is a submodule of N .
- (90) Let R be an integral domain and M an R -module.
- (a) Prove that $\text{Tor}(M)$ is a submodule of M .
 - (b) If M, N are R -modules and $\phi : M \rightarrow N$ is an R -module homomorphism, prove that $\phi(\text{Tor}(M)) \subseteq \text{Tor}(N)$. If ϕ is an isomorphism show that $\phi(\text{Tor}(M)) = \text{Tor}(N)$.
 - (c) Suppose $M \cong N_1 \oplus N_2$ for R -modules N_1 and N_2 . If N_1 is torsion-free and N_2 is torsion, prove that $\text{Tor}(M) \cong N_2$ and $M/\text{Tor}(M) \cong N_1$.
- (91) Let $M_1, \dots, M_n$ be R -modules and let N_i be a submodule of M_i for all $i = 1, \dots, n$. Prove that
- $$\frac{M_1 \oplus \dots \oplus M_n}{N_1 \oplus \dots \oplus N_n} \cong \frac{M_1}{N_1} \oplus \dots \oplus \frac{M_n}{N_n}$$
- (92) If R is a Noetherian commutative ring with $1 \neq 0$ and I is an ideal of R , prove that R/I is Noetherian.