# BASIC COMPREHENSIVE EXAM IN ALGEBRA
# SYLLABUS

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), 7 (omit 7.5), 8 (omit 8.1), 9 (omit 9.6), 10 (omit 10.4, 10.5), 12 (omit 12.3), 13 (omit 13.3, 13.5, 13.6), 15 (omit 15.4, 15.5).

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 $\sigma$ is the $m$-cycle $(a_1\ a_2\ \ldots\ a_m)$, then for all $i \in \{1, 2, \ldots, m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k + i$ is replaced by its least positive residue modulo $m$. Deduce that $|\sigma| = m$.

(7) Let $\sigma$ be the $m$-cycle $(12 \ldots m)$. Show that $\sigma^i$ 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 $\varphi : G \to H$ 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 $\varphi$ 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 $G = < \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} > \subset GL(2; \mathbb{R})$. 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 $\operatorname{lcm}(m, n)$.
(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 $c_1, \ldots, c_r$ are the orders of the centralizers of elements from the distinct conjugacy classes prove that
$$\frac{1}{c_1} + \ldots + \frac{1}{c_r} = 1.$$

(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
$$\operatorname{rad}(I) = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+\},$$
the *radical* of $I$. Prove that $\operatorname{rad}(I)$ is an ideal containing $I$ and that $(\operatorname{rad}(I))/I$ is the nilradical of the quotient ring $R/I$, i.e. $(\operatorname{rad}(I))/I = \mathcal{N}(R/I)$.

(50) Let $R$ be a ring with identity and $I_1, \ldots, I_n$ be $R$-ideals. Show that $R = I_1 + \ldots + I_n$ with $I_j \cap \sum_{i \neq j} I_i = 0$ for every $j$ if and only if $1 = e_1 + \ldots + e_n$ 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 $I_1, \ldots, I_n$ be $R$-ideals with $I_i + I_j = R$ whenever $i \neq j$. Show that $I_1 \cap \ldots \cap I_n = I_1 \cdot \ldots \cdot I_n$.

(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) Verify properties (1) – (10) for $\mathcal{Z}$ and $\mathcal{I}$ given on p. 659 and p. 661 in the Dummit and Foote textbook.
(67) Prove that for ideals $I$ and $J$ of a commutative ring, $\sqrt{I \cap J} = \sqrt{IJ} = \sqrt{I} \cap \sqrt{J}$.
(68) Let $K$ be a field, and let $I = (XY, (X - Y)Z) \subseteq K[X, Y, Z]$. Prove that $\sqrt{I} = (XY, XZ, YZ)$.
(69) Let $I$ be a proper ideal of a commutative ring. Prove that $I$ is a radical ideal if and only if the ring $R/I$ has no nonzero nilpotent elements. (An element $x$ of a ring is nilpotent if $x^n = 0$ for some $n > 0$.)
(70) Prove that if $R$ is a Noetherian ring, then every proper ideal is an intersection of finitely many primary ideals, each of which is primary for a different prime ideal of $R$.
(71) Let $Q$ be a primary ideal of a commutative ring $R$. Let $A, B$ be ideals, and assume $AB \subseteq Q$. Assume that $B$ is finitely generated. Show that $A \subseteq Q$ or there exists some positive integer $n$ such that $B^n \subseteq Q$.
(72) Let $R$ be a commutative ring, and let $M$ be a maximal ideal of $R$. Prove that for $n > 0$, the ideal $M^n$ is $M$-primary. (This is not true in general for non-maximal prime ideals, but you don't have to prove it.)
(73) 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 $M$.
(74) 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 $R$.
(75) Let $I$ be an ideal of the commutative ring $R$, and let $\{M_\alpha\}$ be a collection of $R$-modules. For $N = \oplus_\alpha M_\alpha$, show that $\oplus_\alpha M_\alpha / IM_\alpha$ is isomorphic to $N/IN$ as $R/I$-modules.
(76) Let $F_1 = \oplus_{i=1}^{n} R$ and $F_2 = \oplus_{i=1}^{m} R$ 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.
(77) Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ 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 $T$).
(78) Prove that the constant term of the characteristic polynomial of the $n \times n$ matrix $A$ is $(-1)^n \det(A)$.
(79) Prove that the product of eigenvalues of the $n \times n$ matrix $A$ is $\det(A)$.
(80) Prove that the sum of eigenvalues of the $n \times n$ matrix $A$ is the trace of $A$.
(81) Show that the $F[X]$-module $V_T$ determined by a linear transformation $T : V \to V$ is cyclic if and only if the characteristic polynomial of $T$ is the minimal polynomial of $T$.
(82) 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.)
(83) Find all possible rational canonical forms of $4 \times 4$ matrices $A$ over $\mathbb{R}$ satisfying $A^3 = I$.