Format and topics
Exam 2, Math 128B

General information. Exam 2 will be a timed test of 75 minutes, covering Chapters 16–20 of the text. No books, notes, calculators, etc., are allowed. Most of the exam will rely on understanding the problem sets and the definitions and theorems that lie behind them. If you can do all of the homework, and you know and understand all of the definitions and the statements of all of the theorems we've studied, you should be in good shape.

You should not spend time memorizing proofs of theorems from the book, though understanding those proofs does help you understand the theorems. On the other hand, you should defintely spend time memorizing the *statements* of the important theorems in the text.

The exam will contain the same four types of questions as the previous one. (Remember to be as specific as possible on the true/false questions.) The exam will not be cumulative, per se, as there will not be any questions that only concern material before Ch. 16. However, it will be assumed that you still understand the previous material; for example, it will be assumed that you know what rings and ideals are, what the characteristic of a ring is, what $\mathbf{R}[x]$ is, and so on.

Definitions. The most important definitions we have covered are:

Ch. 16	polynomials over R	$R[x]$
	degree of $f(x)$	leading coefficient of $f(x)$
	monic polynomial	constant polynomial
	quotient, remainder	zero/root of a polynomial
	multiplicity of a zero/root	primitive nth root of unity
	principal ideal domain	
Ch. 17	irreducible over D	reducible over D
	content of a polynomial	primitive polynomial
Ch. 18	associates	irreducible
	prime	norm $N(x)$
	unique factorization domain (UFD)	ascending chain condition
	Noetherian domain	Euclidean domain
Ch. 19	vector space over a field F	vector
	scalar	vector addition
	scalar multiplication	subspace
	linear combination	span (noun) of $\{v_1, \dots, v_k\}$
	span (verb)	linearly dependent
	linearly independent	basis
	dimension	finite-dimensional
	infinite-dimensional	
Ch. 20	extension field	splitting field for $f(x)$ over E
	$F(a_1, \dots, a_n)$	derivative
	multiple zeros	perfect field

Examples. You will also need to be familiar with the key properties of the main examples we have discussed. The most important examples we have seen are:

Ch. 16 Polynomials are not just functions: e.g., x^3 and x^5 in $\mathbf{Z}_3[x]$. Multiplication in $R[x]$; division with remainder in $R[x]$. Roots of $x^n - 1$.

Ch. 17 Examples comparing reducibility over $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{Z}_p$ (PS05, pp. 305–306). Examples of proving polynomials irreducible over $\mathbf{Q}$ (pp. 308–310). Constructing finite fields (pp. 312–313).

Ch. 18 Non-UFD's and bad factorizations: $\mathbf{Z}[\sqrt{d}]$ for $d = -3, -5, -6, +5$; irreducibles that are not prime in the same rings. Ring with element that cannot be factored into irreducibles: $\mathbf{Z}[\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \dots]$. $\mathbf{Z}[x]$ and $F[x, y]$ are UFD's that are not PID's; $\mathbf{Z}[(1 + \sqrt{-19})/2]$ is a PID that is not an ED; $\mathbf{Z}$ and $F[x]$ are ED's.

Ch. 19 Vector spaces over various fields (p. 346); if F is a subfield of E, then E is a vector space over F. Examples of subspaces; subsets that are not subspaces.

Ch. 20 Adjoining elements to find a zero for $f(x)$ (p. 355). Examples of splitting fields (pp. 356, 358, 360, 362; PS07 and other problems).

Theorems, results, algorithms. The most important theorems, results, and algorithms we have covered are listed below. You should understand all of these results, and you should be able to state any theorem clearly and precisely. You don't have to memorize theorems by number or page number; however, you should be able to state a theorem, given a reasonable identification of the theorem (either a name or a vague description).

Ch. 16 D integral domain $\Rightarrow$ $D[x]$ integral domain. Division Algorithm for $F[x]$; corollaries: Remainder Theorem, Factor Theorem, degree n has at most n zeros. $F[x]$ is a PID. An ideal in $F[x]$ is generated by a term of lowest degree.

Ch. 17 Reducibility test for degree 2 and 3; finding irreducibles by making list of irreducibles of degree 1, 2, 3,.... Gauss' Lemma; reducible over $\mathbf{Q}$ implies reducible over $\mathbf{Z}$. Reducibility tests: Mod p, Eisenstein. pth cyclotomic is irreducible. $\langle p(x)\rangle$ maximal iff $p(x)$ irreducible iff $F[x]/\langle p(x)\rangle$ is a field. $\mathbf{Z}[x]$ is a UFD.

Ch. 18 Prime elements are always irreducible, but not converse. ED implies PID; PID implies Noetherian (ascending chain condition) and every irreducible is prime; Noetherian and every irreducible imply UFD. Analogies between $\mathbf{Z}$ and $F[x]$. If D is a UFD, then $D[x]$ is a UFD.

Ch. 19 Invariance of dimension (basis size). Spanning set can be contracted to a basis (Ch. 19 #9); linearly independent set in a finite-dimensional vector space can be expanded to a basis (PS06). Dimension is size of largest linearly independent set and smallest spanning set.

Ch. 20 Fundamental Theorem of Field Theory. Every $f(x)$ has a splitting field. For $p(x)$ irreducible, $F(a) \approx F[x]/\langle p(x)\rangle \approx F(b)$. Splitting fields are unique. Properties of the derivative. Derivative criterion for multiple zeros. Finite fields are perfect. Irreducible polynomials over perfect fields do not have multiple zeros (Thm. 20.5).

Not on exam. (Ch. 17) Weird dice (pp. 314–316). (Ch. 18) Historical discussion of Fermat's Last Theorem. (Ch. 20) Thm. 20.6; Thm. 20.9 and Corollary.

Good luck.