Format and topics for exam 2
Math 127

General information. Exam 1 will be a timed test of 65 minutes, covering Sections 5.2–5.6, 6.1–6.4, and 7.1–7.7 of the class notes/text. More to the point, the exam will cover the portions of PS05–09 coming from Chs. 5–7 and the ideas contained therein. You are allowed

ONE PAGE OF HANDWRITTEN NOTES

and no other aids (books or calculators).

As before, 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 learning proofs of theorems from the book, except the ones assigned on homework. On the other hand, you should defintely spend time learning the *statements* of the important theorems in the text.

Other than the one page of handwritten notes, Exam 2 will follows the same ground rules as Exam 1 did. There will be four of the same types of questions: computations, proofs, explanations/problem solving, and true/false with justification. (Because notes are allowed, there will be no statements of definitions/theorems.)

Definitions. The most important definitions and symbols we have covered are:

5.3	F^n	vector
	zero vector	scalar
	vector addition	scalar multiplication
	subspace	linear combination
	coefficients of a lin. comb.	trivial lin. comb.
	nontrivial lin. comb.	span (noun)
	span (verb)	spanning set
	linearly dependent	linear dependency
	linearly independent	basis
	dimension	coordnates
5.4	$n \times k$ matrix	matrix addition
	scalar multiplication	row-column product
	dot product	matrix-vector product
	matrix product	column space
	$\mathrm{Col}(A)$	nullspace
	$\mathrm{Null}(A)$	
5.5	linear equation	system of linear equations
	augmented matrix of a linear system	solution space
	homogeneous	matrix of a linear system
	REF	leading 1
	pivot column	RREF
	pivot variable	free variable
	elementary row operations	Gaussian reduction
	rank	nullity
5.6	maximal linearly independent set	
6.1	parity check code of length $n+1$	repetition code of length n
6.2	bit	bitstring of length n
	code	codeword
	binary linear code of length n	standard framework
	encoding	decoding
	correct	read
	generator matrix	parity check matrix
	syndrome	

6.3	Hamming 7-code	$\mathcal{H}_7$
	Hamming 8-code	$\mathcal{H}_8$
6.4	$[n, k, d]$ binary linear code	Hamming distance
	Hamming weight	Hamming path of length k
	metric	
7.1	ideal	principal ideal generated by a
	(a)	ideal generated by a and b
	(a, b)	
7.2	additive coset	$r + I$
	coset representative	quotient ring
	R/I	
7.3	reduced representative	root of $m(x)$
	$F[\alpha]$, α is a root....	
7.4	PID	minimal polymomial
7.5	homomorphism	isomorphism
	automorphism	
7.6	order (of a ring/field)	characteristic of R
	multiplicative group $F^\times$	cyclic subgroup $\langle\alpha\rangle$
	cyclic	order (of an element)
	$\mathbb{F}_q$	

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 correctly. More precisely, you should be able to state any of the theorems, given a reasonable identification of the theorem (either its name or a vague description).

Sect. 5.2 Three-cartoon summary of linear algebra.

Sect. 5.3 Span is a subspace (Thm. 5.3.7); a basis gives unique coordinates (Thm. 5.3.13).

Sect. 5.4 Algebraic properties of matrix multiplication (Thm. 5.4.7). Nullspaces are subspaces (Thm. 5.4.9); columns are linearly independent if and only if nullspace is 0 (Thm. 5.4.10); $\mathbf{b}$ is in $\mathrm{Col}(A)$ if and only if $A\mathbf{x} = \mathbf{b}$ has a solution.

Sect. 5.5 Solving a homogeneous (Alg. 5.5.3) or inhomogeneous (Alg. 5.5.4) linear system in RREF. RREF gives basis for nullspace (Thm. 5.5.7). Gaussian reduction (Alg. 5.5.9). Columns linearly independent if and only if all pivot (Cor. 5.5.12). Finding a basis for $\mathrm{Col}(A)$ (Thm. 5.5.14). Rank-nullity (Cor. 5.5.16).

Sect. 5.6 Comparison Theorem 5.6.2, Dimension Theorem 5.6.3, dim is min span/max linearly independent (Cor. 5.6.4). Maximal linear independent set is a basis (Thm. 5.6.6); bases always exist (Cor. 5.6.7). Bigger subspace has bigger dimension (Cor. 5.6.8).

Sect. 6.1 Majority logic for repetition code (6.1.3).

Sect. 6.3 Decoding $\mathcal{H}_7$ (Alg. 6.3.2); $\mathcal{H}_7$ corrects 1 error Thm. 6.3.4. $\mathcal{H}_8$ corrects 1 error, detects 2 (Thm. 6.3.6).

Sect. 6.4 Hamming distance is shortest Hamming path (Thm. 6.4.8), is translation invariant (Cor. 6.4.9), is a metric (Thm. 6.4.11). Nearest-neighbor error correction (Alg. 6.4.12). Nearest neighbor corrects $\lfloor (d-1)/2 \rfloor$ errors, detects $\lfloor d/2 \rfloor$ errors.

Sect. 7.2 "Same coset" descriptions (Thm. 7.2.4). R/I is a ring.

Sect. 7.3 Reduced representatives in $F[x]/I$ (Thm. 7.3.2); units in $F[\alpha]$ (Cor. 7.3.7); when is $F[x]/(m(x))$ a field (Cor. 7.3.8).

Sect. 7.4 Euclidean domains are PIDs (Thm. 7.4.2), computing minimal polynomial of $(a(x), b(x))$ (Thm. 7.4.5). PIDs have unique factorization (Thm. 7.4.6).

Sect. 7.5 Homomorphisms preserve 0, negatives (Thm. 7.5.4). Composition of homomorphisms is a homomorphism (Thm. 7.5.5); inverse of an isomorphism is a homomorphism (Thm. 7.5.7). Automorphisms and zeros (Thm. 7.5.11); complex roots of a real polynomial come in conjugate pairs (Cor. 7.5.12).

Sect. 7.6 Finite field facts: prime characteristic (Thm. 7.6.5); multiplicative group $F^\times$ cyclic; every $\alpha \in \mathbb{F}_q$ is a root of $x^q - x$; constructed by $\mathbb{F}_p[x]/m(x)$; there exists a unique field $\mathbb{F}_q$ of order q. Also: Facts about orders (Thm. 7.6.11).

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:

Sect. 5.3 Bitstrings are elements of $\mathbb{F}_2^n$. Subspaces: F^n, zero subspace. Bases for F^n, zero subspace.
Sect. 5.4 Matrix-vector multiplication is linear combination of columns.
Sect. 5.5 Solving equations in RREF. Gaussian reduction.
Sect. 5.6 Calculating: $\mathrm{Col}(A)$, $\mathrm{Null}(A)$, rank, nullity in various situations.
Sect. 6.1 Parity check code, repetition code.
Sect. 6.2 Parity check code by parity check matrix; repetition code from generator matrix.
Sect. 6.3 Encoding and decoding in $\mathcal{H}_7$.
Sect. 6.4 $[n, k, d]$ stats of: parity check code, repetition code, $\mathcal{H}_7$, $\mathcal{H}_8$. Hamming distance.
Sect. 7.1 Examples of ideals: Even integers, R, $\{0\}$, (m), $(m(x))$, substitution kernel
Sect. 7.2 Cosets of (2), (5). $\mathbb{Z}/(2)$ (Exmp. 7.2.10).
Sect. 7.3 Computation in $\mathbb{F}_2[x]/(x^4 + x + 1)$. Inversion in $\mathbb{F}_2[x]/m(x)$.
Sect. 7.5 Canonical homomorphism $\varphi : R \to R/I$, substitution homomorphism. Complex conjugation, induced homomophrism.
Sect. 7.6 Characteristics of $\mathbb{Z}/(m)$, $\mathbb{F}_q[x]/(m(x))$. Primitive elements and orders of other elements in $\mathbb{Z}/7$ (Exmp. 7.6.12).
Sect. 7.7 Working in $\mathbb{F}_8$ and $\mathbb{F}_{16}$.

Other. You should have a working familiarity with techniques and strategies for proof and logic tips, to the extent that we have done proofs in the homework. You should also review how to prove that a set is closed under a given operation (Section 1.3.4).

Not on exam. Ch. 4; Section 5.1.

Good luck.