

Format and topics for exam 3
Math 127

General information. Exam 3 will be a timed test of 75 minutes, covering Sections 7.1–7.6 and 8.1–8.5 of the class notes/text. While not assigned explicitly, you may also find the worked examples of 7.7 to be helpful. More to the point, the exam will cover the material in PS07–09 and the ideas contained therein.

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 memorizing proofs of theorems from the book, though understanding those proofs does help you understand the theorems. On the other hand, you should definitely spend time memorizing the *statements* of the important theorems in the text.

Exam 3 will follow the usual ground rules. In particular, no books, notes, or calculators are allowed, and there will be the same four types of questions: computations, statements of definitions and theorems, proofs, explanations/problem solving, and true/false with justification.

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

7.1	ideal (a) (a, b)	principal ideal generated by a ideal generated by a and b
7.2	additive coset coset representative R/I	$r + I$ quotient ring
7.3	reduced representative $F[\alpha]$ where α is a root of $m(x)$	root of $m(x)$
7.4	PID	minimal polynomial
7.5	homomorphism automorphism	isomorphism
7.6	order (of a ring/field) multiplicative group F^\times cyclic order (of an element)	characteristic of R cyclic subgroup $\langle \alpha \rangle$ primitive element $\mathbf{F}_q, GF(q)$
8.1	Hamming n -code ($n = 2^r - 1$)	
8.2	cyclic code	polynomial notation
8.3	generator polynomial of a cyclic code	
8.4	extension field Frobenius automorphism Frobenius orbit	factoring over a field F minimal polynomial
8.5	BCH code BCH code given by E, α, δ	designed distance

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. 7.1 Ideals are closed under negatives (Thm. 7.1.9).

Sect. 7.2 “Same coset” descriptions (Thm. 7.2.4). R/I is a ring (Thm. 7.2.11).

Sect. 7.3 Reduced representatives in $F[x]/I$ (Thm. 7.3.2); units in $F[\alpha]$ (Cor. 7.3.7); when $F[x]/(m(x))$ is 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. 7.5.7). Composition of homomorphisms is a homomorphism (Thm. 7.5.8); inverse of an isomorphism is a homomorphism (Thm. 7.5.10). Automorphisms and zeros (Thm. 7.5.13).
- Sect. 7.6** Five Facts for Finite fields: prime characteristic (Thm. 7.6.5); multiplicative group F^\times is cyclic; every $\alpha \in \mathbf{F}_q$ is a root of $x^q - x$ (Cor. 7.6.14); constructed by $\mathbf{F}_p[x]/m(x)$; there exists a unique field \mathbf{F}_q of order q . Facts about orders (Thm. 7.6.11): Max order implies cyclic, Order of a Power Formula, Lagrange's Theorem.
- Sect. 7.7** Worked examples of finite fields: \mathbf{F}_8 and \mathbf{F}_{16} .
- Sect. 8.2** Cyclic codes are ideals (Thm. 8.2.7).
- Sect. 8.3** Cyclic codes are principal ideals $g(x)$, where $g(x)$ divides $x^n - 1$. Basis and dimension for cyclic code ($g(x)$).
- Sect. 8.4** Facts about the Frobenius automorphism (Thm. 8.4.7). Minimal polynomial for $\beta \in E$ (Thm. 8.4.9). Orbit Theorem 8.4.13. Number of elements in a Frobenius orbit divides e , where $|F| = 2^e$ (Thm. 8.4.17).
- Sect. 8.5** BCH Theorem 8.5.1. BCH Algorithm 8.5.3.

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. 7.1** Examples of ideals: Even integers, R , $\{0\}$, (m) , $(m(x))$, substitution kernel.
- Sect. 7.2** Cosets of (2) , (5) . $\mathbf{Z}/(2)$ (Exmp. 7.2.10).
- Sect. 7.3** Computation in $\mathbf{F}_2[x]/(x^4 + x + 1)$. Inversion in $\mathbf{F}_2[x]/m(x)$.
- Sect. 7.5** Canonical homomorphism $\varphi : R \rightarrow R/I$, substitution homomorphism, induced homomorphism. Non-examples of homomorphisms (Exmp. 7.5.5). Complex conjugation.
- Sect. 7.6** Characteristics of $\mathbf{Z}/(m)$, $\mathbf{F}_q[x]/(m(x))$. Primitive elements and orders of other elements in $\mathbf{Z}/7$ (Exmp. 7.6.12–7.6.14).
- Sect. 8.1** Hamming n -codes, $n = 2^r - 1$.
- Sect. 8.2** Cyclic codes with all vectors written out: Parity check length 4 and Hamming 7-code (Exmps. 8.2.3–8.2.4).
- Sect. 8.3** Cyclic codes described in terms of generators: parity check, repetition, \mathcal{H}_7 , \mathcal{H}_n , Golay 23-code.
- Sect. 8.4** Minimal polynomial for $\alpha \in \mathbf{F}_q$. Factoring over different fields F (Exmps. 8.4.3, 8.4.4). Orbits in \mathbf{F}_8 .
- Sect. 8.5** BCH examples (Exmp. 8.5.5–8.5.9).

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. In particular, you should review how to prove that a set is closed under a given operation, and how to prove that a subset I of a ring R is an ideal.

Not on exam. Kernels (7.5.15–7.5.17). Proof of BCH Theorem (Lem. 8.5.11).

Good luck.