Modern algebra II, Review problems and topics for the final exam, part 2.

One recommendation is to go over homework problems over the span of the semester (homework 1-12; a significant fraction of final exam problems will be similar to those on the homework. Beyond that, here are other sample problems.

1. Rings, subrings, ideals. Quotient rings. Commutative and noncommutative rings. Some of the possible questions:
(a) Which of the following rings are (1) commutative, (2) integral domains, (3) fields

$$\mathbb{Q}[x]/(x-5),\ \ \mathbb{Q}[x,y]/(xy),\ \ \mathbb{Z}/(23),\ \ \mathbb{Q}[x]/(x^2)\times\mathbb{Q},\ \ \mathbb{R}[x]/(x^2+x+8),$$
$$\mathbb{F}_4[x]/(x^2+x+1),\ \ \mathbb{Q}[x],\ \ \mathbb{Z}[x],\ \ \mathbb{F}_4[x]/(x^3+x+1)?$$

(b) Which of the following rings have ideals that are not prime?

$$\mathbb{Z}/(4),\ \ \mathbb{Z},\ \ \mathbb{F}_2[x]/(x^4+x+1),\ \ \mathbb{Q},\ \ \mathbb{F}_p\times\mathbb{F}_p.$$

(c) Compute sum $I+J$, product IJ and intersection $I\cap J$ of ideals $I=(x^2+x)$ and $J=(x^3+1)$ of $\mathbb{F}_2[x]$. For more practice, you can choose other rings and ideals in them.

(d) Can you give an example of a noncommutative ring with 8 elements?

(e) Suppose I is an ideal in a commutative ring R and S a subring of R. Prove that $J=I\cap S$ is an ideal of S. What's the relation between quotient rings R/I and S/J?

(f) Show that four-element rings $\mathbb{F}_4, \mathbb{F}_2\times\mathbb{F}_2, \mathbb{Z}/4, \mathbb{F}_2[x]/(x^2)$ are pairwise non-isomorphic. Are there any four-element rings R that are not isomorphic to any of these rings?

(g) Review the construction of a quotient field $Q(R)$ of an integral domain R. Why is the natural map $R\longrightarrow Q(R)$ an inclusion of rings?

(h) What goes wrong when one tries to define ideals of a noncommutative ring R? (Nothing does, but there are several types of ideals: left, right, and 2-sided.) How would you define an ideal I in a noncommutative ring R to make the quotient R/I a ring?

2. Take a vector space V of dimension n over a finite field $\mathbb{F}_p$.
(a) Count the number of bases of V as a vector space over $\mathbb{F}_p$.

(b) How many one-dimensional subspaces does V have?

(c) How many k-dimensional subspaces does V have (assume $k\leq n$).

First try this on your own. You can read a solution on Stackexchange:
`https://math.stackexchange.com/questions/1715249/the-number-of-subspaces-over-a-finit`

3. Notion of homomorphism. Can you classify homomorphisms from the ring $\mathbb{Z}[x]$ to a ring R? Are there any homomorphisms from $\mathbb{Z}/(20)$ to $\mathbb{Z}/(10)$?

What about homomorphisms from $\mathbb{Z}/(10)$ to $\mathbb{Z}/(20)$? Why is any homomorphism from a field F to a ring R injective (assume R is not the zero ring)? Why is any homomorphism from a finite extension E of $\mathbb{Q}$ to itself is an isomorphism? (Same question for homomorphisms $F \longrightarrow F$, where F is a finite field). You may get a question: among the following maps of rings, select those that are homomorphisms, similar to problem 2 on homework 3. In our definition of homomorphisms, 1 always goes to 1.

4. Idempotents in commutative rings and direct product decomposition. Show that under a ring homomorphism an idempotent is mapped to an idempotent. Idempotent decomposition of $\mathbb{Z}/(nm)$ for relatively prime n and m (Chinese Remainder Theorem).

5. Testing whether polynomials in $F[x]$ are irreducible, where F is a field, including for polynomials over a finite field and polynomials of degree at most 3. For the latter, we just need to see if a root exists. Gauss lemma about factorization of polynomials over $\mathbb{Z}$ and $\mathbb{Q}$ (see Rotman).

6. Computing *gcd* and *lcm* of polynomials, including over finite fields (see homework examples). Relation between *gcd* and *lcm* of polynomials and the sum and intersection of principal ideals that they generate.

7. Construction of finite fields via irreducible polynomials (see examples in homework and midterm) and as the splitting field of $x^q - x$. Symmetries of finite fields (action of Frobenius). Properties of Frobenius and binomial coefficients modulo p (additivity of taking the p-th power). Orbits of Frobenius acting on a finite field. For practice, classify irreducible degree 4 polynomials over $\mathbb{F}_2$. Why are the fields we get from these polynomials isomorphic? Advanced question (we did not discuss it in the course, but it's in Rotman): derive a formula for the number of monic irreducible polynomials of degree n over $\mathbb{F}_p$ (start with the case when n is prime).

8. Field extensions, degree of an extension. Construction of extensions via $F[x]/(f(x))$, where $f(x)$ is irreducible. Degree formula for intermediate fields $F \subset K \subset E$. Algebraic versus transcendental elements. Sum and product of algebraic elements is algebraic. Find the irreducible polynomial of $\alpha = i + \sqrt{6}$ over various fields: $\mathbb{Q}$, $\mathbb{Q}[\sqrt{6}], \mathbb{C}$ (question 4 on homework 6 is similar; go over other questions on that homework as well).

9. Eisenstein criterion and its use in showing that various polynomials are irreducible. Fields of characteristic p and examples of inseparable polynomials. (see questions in homework 7).

10. Automorphisms of fields and Galois groups. Automorphisms of rings. Splitting field extensions. Computations of Galois groups. Galois groups in the finite fields case. Galois groups of extensions that involve square roots, $\mathbb{Q}[\sqrt{p}, \sqrt{q}]$, for instance. Galois groups of degree 3 extensions (also see part 1).

(a) Can you classify all automorphisms of the ring (a) $\mathbb{Z}$, (b) $\mathbb{Z}[\frac{1}{2}]$, (c) $\mathbb{Q}[x]$, (d) $\mathbb{F}_2[x]/(x^3)$, (e) $\mathbb{F}_p \times \mathbb{F}_p$?

11. Galois Main Theorem. Correspondence between subfields and subgroups. Examples (if you have time, work through the splitting field of x^4-2 example in Friedman, Notes on Galois theory, II, with a full correspondence between subgroups and subfields). Solvable groups and solvability of equations in radicals.