1 List of results

You are reminded that the best way to prepare for the exam is to thoroughly *understand* the material seen in class, and to solve the exercises. This will allow you to be able to tackle the the exam without relying too much on memory.

The main purpose of this document is to list the important results whose proofs would be too long to be reconstructed on the spot unless one is very familiar with them, and to clarify when a related result may be quoted without proof. But keep in mind that you should still be able to place them in their context, apply them as the need arises, and also reconstruct minor (possibly related) results independently. You are also strongly advised to attempt the exercises.

Unless otherwise indicated below, when proving a certain result, any required previous result may be quoted without proof.

1. Theorem 1 (R^* is a group), including Lemma 6.
2. Theorem 2 (finite IDs are fields) (without the proof of Lemma 7)
3. Theorem 3 (n is prime iff $\mathbb{Z}_n$ is a field), including proof of claim
4. Theorem 4 (subring test)
5. Lemma 11 (ideal test)
6. Theorem 5 (factor rings), including proof of part (b) (as in earlier Claim B)
7. Proposition 1 (field iff no proper ideal)
8. Theorem 6 (one-to-one correspondence between ideals)
9. Proposition 2 (R/I is a field iff I is maximal)
10. Theorem 7 (isomorphisms), including Lemma 10, but Lemma 13a may be quoted without proof
11. Lemma 14 (division property of Gaussian integers)

12. Theorem 8 (ERs are PIDs)
13. Theorem 9 (Euclidean algorithm)
14. Theorem 10 (irreducible iff maximal)
15. Theorem 11 (PIDs are UFDs), including Lemmas 18, 19 and Exercise (xxviii)