MATH 340 Final Examination

Thursday December 9th, 12:00-15:00, AQ 3153

There are 12 questions. Attempt all questions.
The total number of marks is 120 and you have 180 minutes.
This examination is closed book.
No calculators or electronic devices permitted.

Sections covered
Chapter 1: 1.1-1.7, 1.10-1.11 (no bar codes)
Chapter 2: 2.1-2.2, 2.4-2.13 (no vector spaces, no error correcting codes)
Chapter 3: 3.1

Please especially review

1. The extended Euclidean algorithm in $\mathbb{Z}$ (page 22) and for $F[x]$ and applications.

2. The definition of Ring, Field, zero divisor, integral domain, and Group, and examples of each.

3. How to construct a finite field with $q = p^n$ elements using an irreducible polynomial in $\mathbb{Z}_p[x]$ and how to do arithmetic in the field using equivalence classes. E.g. construct the addition and multiplication table for $G = \mathbb{Z}_2[y]/(y^2 + y + 1)$ and find all primitive elements in G.

4. The statement and proof of Euler's theorem and Fermat's theorem for $\mathbb{Z}_n$ (section 1.11) and Fermat's theorem for $GF(p^n)$ (Lemma 2.9.1).