Math 151 **Review sheet** Spring 2004

1. **Definitions, examples, basic properties:**
   (a) Algebraic structures
      - set
      - group (abelian)
      - ring (commutative, commutative with identity)
      - integral domain
      - field
      - direct sum / product of two sets, groups, or rings
      - integer numbers (quotient, remainder, primes, gcd, lcm, congruence modulo n)
      - polynomials (monic, irreducible, quotient, remainder, gcd, lcm)

   (b) Substructures
      - subset
      - subgroup
      - subring
      - ideal (zero, proper, prime, maximal)
      - subfield

   (c) Functions
      - well-defined
      - one-to-one (injection)
      - onto (surjection)
      - one-to-one correspondence (bijection)
      - permutation
      - homomorphism
      - isomorphism
      - kernel
      - image
      - inverse function
      - composition

2. **Important theorems** (a star indicates that you should know a proof)
   - Division algorithm (Th 1.1.3, p. 7)
   - GCD as a linear combination (Th 1.1.6, p. 9)
   - Fundamental theorem of arithmetic (Th 1.2.6, p. 18)
   - (*) Euclid's theorem (Th 1.2.7, p. 19)
   - (*) Inverse of an integer modulo n (Prop 1.3.4, p. 26)
   - Solution to a congruence $ax \equiv b \pmod{n}$ (Th 1.3.5, p. 26)
   - (*) Chinese remainder theorem (Th 1.3.6, p. 29)
   - Lagrange's theorem (Th 3.2.10, p. 99)
   - Decomposiotion of a finite abelian group (Th 3.5.4, p. 123)
   - Cayley's theorem (Th 3.6.2, p. 127)
   - (*) Fundamental homomorphism theorem for groups (Th 3.8.8, p. 152)
   - (*) Remainder theorem (Th 4.1.9, p. 167)
   - Root of a polynomial (Cor 4.1.11, p. 169)
   - Unique factorization (Th 4.2.9, p. 178)
   - Eisenstein's irreducibility criterion (Th 4.3.6, p. 184)
   - $F[x]/ < p(x) >$ is a field if $p(x)$ is irreducible (Th 4.4.6, p. 190)
   - Kronecker's Theorem (Th 4.4.8, p. 191)
   - (*) Fundamental homomorphism theorem for rings (Th 5.2.6, p. 215)
   - Factor ring (Prop 5.3.9, p. 224)