Math 151 **Review sheet** Fall 2008

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

   (b) Substructures
   - subset
   - subgroup
   - subring
   - subfield

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

2. **Important theorems** (a star indicates that you should know a proof)
   - Division algorithm (Th 1.1.3, p. 6)
   - GCD as a linear combination (Th 1.1.6, p. 8)
   - Fundamental theorem of arithmetic (Th 1.2.7, p. 18)
   - (*) Euclid's theorem about prime numbers (Th 1.2.8, p. 20)
   - (*) Inverse of an integer modulo n (Prop 1.3.4, p. 27)
   - Solution to a congruence $ax \equiv b \pmod{n}$ (Th 1.3.5, p. 28)
   - (*) Chinese remainder theorem (Th 1.3.6, p. 31)
   - Lagrange's theorem (Th 3.2.10, p. 110)
   - Decomposiotion of a finite abelian group (Th 3.5.5, p. 138)
   - Cayley's theorem (Th 3.6.2, p. 142)
   - (*) Fundamental homomorphism theorem for groups (Th 3.8.9, p. 172)
   - (*) Remainder theorem for polynomials (Th 4.1.9, p. 188)
   - Root of a polynomial (Cor 4.1.11, p. 189)
   - Unique factorization (Th 4.2.9, p. 199)
   - $F[x]/ < p(x) >$ is a field if $p(x)$ is irreducible (Th 4.3.6, p. 206)
   - Kronecker's Theorem about an extension field (Th 4.3.8, p. 207)
   - Eisenstein's irreducibility criterion (Th 4.4.6, p. 214)
   - Fundamental homomorphism theorem for rings (Th 5.2.6, p. 244)