Math 3140 Fall 2016 - Review

1. **Symmetries and modular arithmetic.**
   (1) rotations, reflections as invertible matrices (1.4) and permutations (1.5), cycle notation and cycle structure, order of permutations (1.5)
   (2) ring $\mathbb{Z}_n$, gcd, Euclidean algorithm, Bezout's coefficients (1.7), units in $\mathbb{Z}_n$, Euler's Theorem, Fermat's Little Theorem (1.9), RSA (1.12)

2. **Groups.**
   (1) axioms (1.10), uniqueness of identity and inverses (2.1), subgroups, order of elements, generators, cyclic groups (2.2) homomorphism, isomorphism (2.2), Cayley's Theorem
   (2) general linear groups, symmetric groups S_n, dihedral groups D_{2n} with generators and relations, groups of order p^2 and pq up to isomorphism (5.)
   (3) cosets, Lagrange's Theorem (2.5), index
   (4) kernel, image of homomorphisms (2.4), abelian group, center (2.5), conjugacy, normal subgroups, quotient group (2.7), Homomorphism Theorem, Correspondence Theorem (2.7)
   (5) direct products (3.1), Fundamental Theorem of finitely generated abelian groups (3.6)
   (6) group actions, orbits, transitivity, stabilizer, fixed points (5.1), Orbit-Stabilizer Theorem (5.1.14), counting permutations of fixed cycle structure (5.1), counting colorings, Burnside-Frobenius Lemma (5.2)
   (7) group structure, conjugacy classes, class equation, p-groups have non-trivial center (5.4)
   (8) Sylow subgroups, First Sylow Theorem (with proof), Second and Third Sylow Theorem (without proof)

3. **Rings.**
   (1) axioms, commutative ring with 1, units, field (6.1), subring, (unital) ring homomorphisms, kernel, ideal (6.2) quotient ring, Homomorphism Theorem for rings (6.3), direct product of rings, Chinese Remainder Theorem (1.11.7)
   (2) matrix ring $R^{n\times n}$, polynomial ring $R[x]$, fields $\mathbb{Z}_p$ (p prime), $\mathbb{Q}, \mathbb{R}, \mathbb{C}$