Review for Final

Go over everything on the midterm review sheet.

Well ordering principal and mathematical induction, Division algorithm, Fundamental theorem of arithmetic

Equivalence relations and equivalence classes and partitions

Groups and abelian groups, symmetries of a polygon, dihedral groups, order of a group and order of an element of a group.

$Z(G)$, The center of a group. Show that for a given group G, if $G/Z(G)$ is cyclic, then G is abelian.

Subgroups and normalizers and centralizers thereof

The Lagrange coset theorem and its consequence that the order of a subgroup divides the order of a group.

If a is in a group G, $< a >$ is the subgroup generated by a and $|a|$ is the order of a.

Cyclic groups such as Z_n. a, an element of Z_n generates Z_n iff $gcd(n, |a|) = 1$. Z_n is also a ring under multiplication mod n. It has units $U(n)$.
$U(n) = \{x \in Z_n | \gcd(x, n) = 1\}$ $U(st) \cong U(s)U(t)$ if $\gcd(s, t) = 1$

Permutation groups and cycles in them. Disjoint cycles commute. Odd and even permutions. Alternating groups

Normal subgroups and factor (or quotient) groups

Homomorphisms and their kernels, Isomorphisms, Cayley's theorem that every group is isomorphic to a subgroup of some group of permutations, Automorphisms and inner automorphisms.

Fundamental Theorem of Finite Abelian Groups (without proof)

Let p be a prime greater than 2. Show that all groups of order p are cyclic, Show that all groups of order $2p$ are cyclic or dihedral.

Internal and external direct products of groups. Show $Z_n \times Z_m$ is cyclic iff $\gcd(m, n) = 1$. Prove that $U(st) \cong U(s) \times U(t)$ if s and t are relatively prime.

Rings, Integral Domains and Fields

Zero Divisors. Prove that a finite integral domain must be a field.x

Ideals and Principal Ideals, Polynomial rings, and the degree of a polynomial.

Factor or quotient rings: R/I where I is an ideal in the ring R

Maximal Ideals, Prime ideals, R/I in each case

Quotient field of an integral domain, construction of rationals from integers

Characteristic of a ring and of a field

Division algorithm in Z and in $F[x]$, where F is any field

Content of a polynomial in $Z[x]$, primitive polynomial, Gauss lemma

Reducibility in $Z[x]$ and in $Q[x]$.

Mod p irreducibility tests and Eisenstein's criterion.

Let $p(x)$ be a polynomial in $F[x]$. Prove that $< p(x) >$ is a maximal ideal iff $p(x)$ is irreducible.

Define principle ideal domains and unique factorization domains. Show that a PID is a UFD, but not conversely.

Unique factorization in $Z[x]$.

Prove that a principle ideal domain satisfies the ascending chain condition.