Math 546
Final Exam Review

Definitions

Be able to define and use the following terms.

group	identity	inverse
subgroup	normal subgroup	Kernel of a homomorphism
semigroup	Well Ordering Principle	$\phi(A)$ where A is a subset of the group G, and ϕ is a homomorphism.
subgroup	Abelian group	cyclic group
homomorphism	homomorphic image	isomorphism
automorphism, Aut(G)	AB where A and B are subsets of the group G.	[G:H], the index of H in G.
left cosets	partition	G/H
automorphism and inner automorphism and Aut(G) and Inn(G).	center of a group	centralizer of an element of a group
equivalence relation	Euler Phi-function $\phi(n)$	The groups $U(n)$, Z_n, S_n, A_n, $GL(2,R)$
idempotent	relatively prime	inner automorphism, Inn(G)
congruence $x \equiv y \bmod n$	greatest common divisor	countable

Important Theorems

Understand, be able to state, and be able to apply the following results
You should be able to *prove* those statements that are followed by a "**(##)**"

Theorem. Every finite semigroup has an idempotent.

Theorem. The greatest common divisor of positive integers n and m is the least positive element in the set $A = \{an + bm : a, b \in Z\}$ **(##)**

Theorem (Cantor). For any set S, there does not exist a function $f : S \to P(S)$ that is onto. Here $P(S)$ denotes the power set of S.

Theorem If H is a normal subgroup of the group G then G/H is a group under the operation $(aH)(bH) = abH$.

Theorem (Cauchy). If G is a finite Abelian group whose order is divisible by a prime p, then G has an element of order p.

Theorem (LaGrange). If H is a subgroup of the finite group G, then the order of H divides the order of G. So, $|G| = |H|[G:H]$, where $[G:H] = \frac{|G|}{|H|}$ is the *index* of H in G.

Corollary If g is an element of the finite group G, then $o(g)$ divides $|G|$. **(##)**

Corollary If the group G has order n, then for any g in G, $g^n = e$. **(##)**

Theorem (Euler) If a is a positive integer that is relatively prime to the positive integer n, then $a^{\phi(n)} \equiv 1 \bmod n$.

Theorem (Fermat) If a is a positive integer that is not divisible by the prime p, then $a^{p-1} \equiv 1 \bmod p$.

Theorem. If $\phi : G \to H$ is a homomorphism from G onto H, and if $K = \ker \phi$, then $G/K \cong H$. Moreover, the mapping $\gamma : G/K \to H$ defined by $\gamma(aK) = \phi(a)$ is an isomorphism. **(##)**

Theorem. A group H is a homomorphic image of the group G if and only if H is isomorphic to G/K for some normal subgroup K of G.

Theorem. Let G be a group, Z the center of G, and $Inn(G)$ the set of all inner automorphisms of G. Then $G/Z \cong Inn(G)$.

Theorem (Cayley) Every group G is isomorphic to a subgroup of S_G.

Theorem If H is *any* subgroup of G, then the relation $a \equiv b \bmod H \Leftrightarrow a^{-1}b \in H$ is an equivalence relation. **(##)**
This relation also has the property that for any element g in G,
(i). $a \equiv b \bmod H \Rightarrow ga \equiv gb \bmod H$ (i.e., 'multiplication' on the left preserves congruences. **(##)**
(ii). If H is a normal subgroup, then $a \equiv b \bmod H \Rightarrow ag \equiv bg \bmod H$. **(##)**

Theorem. For a finite group G, the 'multiplication table' of G is a Latin Square.

Theorem. Let H be a subgroup of the group G. Then each of the following conditions is equivalent to H being a normal subgroup.

(i). For every $h \in H$, $g \in G$, $ghg^{-1} \in H$ (this was our definition of normal).

(ii). For any g in G, $gH = Hg$ (i.e., the left and right cosets are exactly the same.)

(iii). For any g in G, $gHg^{-1} = H$.

(iv). H is the kernel of some homomorphism with domain G.

Theorem. If H is a finite subset of a group G, then H is a subgroup iff it is closed.

Theorem. If G and H are any cyclic groups of order n, then G is isomorphic to H. Consequently, every cyclic group on n elements is isomorphic to Z_n.

Theorem. The only infinite cyclic group (up to isomorphism) is the integers under addition.

Theorem. Every subgroup of a cyclic group is cyclic. **(##)**

Theorem. If $k \in Z_n$ is relatively prime to n, then k generates $(Z_n, +)$.

Theorem. Let a and b be elements of the Abelian group G with $o(a) = n$, $o(b) = m$. If n and m are relatively prime, then $o(ab) = o(a)o(b)$.

Fundamental Properties of homomorphisms.

Theorem Let $\phi : G \to H$ be a homomorphism. Then

(a). $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$ - that's the *definition* of a homomorphism.

(b). $\phi(e_G) = e_H$

(c). $\ker(\phi)$ is a normal subgroup of G. **(##)**

(d). ϕ is 1-1 iff $\ker(f) = \{e_G\}$ **(##)**

(e). If A is an Abelian subgroup of G, then $\phi(A)$ is Abelian as well.

(f). For any x in G, $\phi(x^{-1}) = [\phi(x)]^{-1}$.

(g) If ϕ is onto H and A is a (normal) subgroup of G, then $\phi(A)$ is a (normal) subgroup of H.

(h) H is a normal subgroup of G if and only if $H = \ker(\phi)$ for some homomorphism ϕ.

(i). $\phi : G \to G/H$ defined by $\phi(g) = gH$ is a homomorphism of G onto H and the kernel of ϕ is H.