Midterm Review

1. Set Theory

bijectivity $\iff$ invertibility

equivalence relation: reflexive: $x \sim x$, symmetric: $x \sim y \to y \sim x$, transitive: $x \sim y, y \sim z \to x \sim z$

equivalent classes on X $\iff$ partitions on X

Examples:

- $x \sim y$ if $y^{-1}x \in H$. This construction leads to cosets.
- $x \sim y$ if $y = gxg^{-1}$ for some g. This construction leads to conjugacy classes.

2a. Groups

A group is a nonempty set G with a law of composition $G \times G \to G$, $(g_1, g_2) \mapsto g_1 g_2$, satisfying:

1. Associative: $\forall g1, g2, g3 \in G$, $(g1g2)g3 = g1(g2g3)$
2. Identity: $1 \in G$ s.t. $\forall g \in G$, $g1 = 1g = g$
3. Inverse: $\forall g \in G$, $\exists g^{-1} \in G$ s.t. $gg^{-1} = g^{-1}g = 1$

abelian group: $\forall g_1, g_2 \in G$, $g_1 g_2 = g_2 g_1$, then G is an . $\iff$ multiplication table is symmetric along diagonal

A group G admits the Cancellation Law: $ac = bc \to a = b$

permutation group on X: $P(X) = \{f : X \to X | f \text{ is bijective}\}$

A subgroup H of a group G is a subset of G satisfying:

1. Closure: $\forall a, b \in H \to ab \in H$
2. Identity: $1 \in H$
3. Inverse: $\forall a \in H \to a^{-1} \in H$

subgroup $\iff$ $\forall a, b \in H \to a^{-1}b \in H.$

subgroup of $\mathbb{Z}$: $a\mathbb{Z}$ for some $a \in \mathbb{N}$.

greatest common divisor $\gcd(a, b)$: d such that $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$

relatively prime if their $\gcd(a, b) = 1$, i.e., $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.

relatively prime $\iff$ $ar + bs = 1$ for some $r, s \in \mathbb{Z}$

cyclic group: $G =< g >$ for some $g \in G$

cyclic subgroup: $< x >= \{x^k \in G | k \in \mathbb{Z}\}$.

Prop. Every subgroup of a cyclic group is a cyclic subgroup.

order of a group G: $|G|$ = the number of elements in G

order of an element g: $|g| = | < g > |$.

$$|g| = \begin{cases} \min\{k \in \mathbb{Z} | k > 0, g^k = 1\} & \text{if the set is nonempty and thus has a min} \\ \infty & \text{otherwise} \end{cases}$$

When $|g| < \infty$, $< g >= \{1, g, g^2, ..., g^{|g|-1}\}$.

When $|g| = \infty$, $< g >= \{..., g^{-2}, g^{-1}, 1, g, g^2, ...\}$.

2b. Homomorphisms

homomorphism: $f : G \to G'$ sayisfying $\forall a, b \in G$, $f(ab) = f(a)f(b)$

Properties: $f(1) = 1'$, $f(g)^{-1} = f(g^{-1})$

kernel: $\ker(f) = \{g \in G | f(g) = 1'\}$, normal subgroup of G

image: $Im(f) = \{f(g) \in G' | g \in G\}$, subgroup of G'

injectivity of $f \iff \ker(f) = \{1\}$ trivial

surjectivity of $f \iff Im(f) = G'$

conjugation of $x \in G$ by $g \in G$: the element $gxg^{-1} \in G$. x and gxg^{-1} are conjugate elements.

normal subgroup $N \lhd G$: if $\forall n \in N$, $\forall g \in G$, $gng^{-1} \in N$, it is equivalent to $\forall g \in G$, $gNg^{-1} \subseteq N$, and equivalent to $\forall g \in G$, $gNg^{-1} = N$.

centre: $Z(G) = \{g \in G | gx = xg \text{ for any } x \in G\}$, it is a normal subgroup of G

G is abelian $\iff Z(G) = G$.

isomorphism = bijective homomorphism

automorphism of G: an isomorphism $\phi : G \to G$

group of automorphisms of G, $Aut(G)$: the set of all automorphisms of G with the law of composition to be composition of functions

inner automorphism group of a group G is the subgroup $Inn(G) = \{\phi_g \in Aut(G) | g \in G\}$.

Examples:

- $Aut(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times$
- $Aut(\mathbb{Z}) = \{\pm 1\}$
- $Aut(S_3) = S_3$

3a. Quotients of Groups

cosets: $[g] = \{x \in G | x = gh \text{ for some } h \in H\} = \{gh \in G | h \in H\} = gH$

$aH = bH \iff a \in bH \iff b^{-1}a \in H$

index of subgroup H in G to be the number of left cosets, denoted by $[G : H]$.

Lagrange's Theorem. $|G| < \infty$. $[G : H] = \frac{|G|}{|H|}$.

Cor. $|H|$ divides $|G|$. $|g| = | < g > |$ divides $|G|$.

Cor. $[G:K] = [G:H][H:K]$

Cor. A group of prime order is cyclic. Any subgroup of index 2 is normal.

quotient group G/N: the set of all cosets of a normal subgroup N in G, composition: $(aN)(bN) = abN$.

Example: $K_4 = \{1, a, b, c\}$, $N = \{1, a\} =< a >$, $K_4/N = \{N, bN\} =< bN >$.

Denote $\bar{k} = k + n\mathbb{Z}$, then $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{k-1}\}$. Composition: $\bar{a} + \bar{b} = \overline{a+b}$.

If $\bar{a} = \bar{b}$, we say "a is congruent to b module n", $a \equiv b \pmod{n}$.

Another composition: multiplication $\bar{a}\bar{b} = \overline{ab}$

unit: an element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ if there exists $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ s.t. $\bar{a}\bar{b} = 1$.

Prop. If $\bar{a}, \bar{c}$ are both units of $\mathbb{Z}/n\mathbb{Z}$, then $\bar{a}\bar{c}$ is also a unit.

group of units, $(\mathbb{Z}/n\mathbb{Z})^\times$: the set of all units in $\mathbb{Z}/n\mathbb{Z}$ with multiplication

Example: $\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$

$\bar{a}$ is a unit $\iff$ $\bar{a}$ is a generator for $\mathbb{Z}/n\mathbb{Z}$ $\iff$ $\gcd(a, n) = 1$ $\iff$ $f_a : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $f_a(\bar{x}) = \overline{ax}$ is a automorphism

Eulers's phi function: $\phi(n) = \#\{k \in \mathbb{N} | 1 \le k \le n, \gcd(k, n) = 1\}$.

Examples: $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$

Fermat's Little Theorem: $n \ge 2$, $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Cor. p is a prime. $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Cor. $Aut(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

First Isomorphism Theorem. $f : G \to G'$ is a surjective homomorphism. Then there is a unique homomorphism $F : G/N \to G'$ ($N = \ker(f)$) such that F is an isomorphism and $f = F \circ \pi$ where $\pi : G \to G/N$, $\pi(g) = gN$ is the quotient map.

Cor. $G/\ker(f) \cong \mathrm{Im}(f)$. (force it to be surjective)

Cor. $|G| < \infty$. Then $|G| = |\ker(f)| \cdot |\mathrm{Im}(f)|$.

Cor. $\gcd(|G|, |G'|) = 1$. Then f is trivial, i.e., $\forall g \in G$, $f(g) = 1'$.

3b. Products of Groups

product group, $G \times G'$: the set of all ordered pairs (g, g') where $g \in G$, $g' \in G'$, with law of composition $(g_1, g_1')(g_2, g_2') = (g_1 g_2, g_1' g_2')$.

$G = H \times K$ if $f : H \times K \to G, f(h, k) = hk$ is an isomorphism.

$G = H \times K \iff H \cap K = \{1\}, HK = G$, and $H, K \lhd G$

Prop. cyclic $C_m \times C_n \cong C_{mn} \iff \gcd(m, n) = 1$.

Lemma. If H and K are subgroups of G, with $|H|$ and $|K|$ relatively prime, then $H \cap K = \{1\}$.

4a. Symmetric Groups

cycles & cycle decomposition.

Computational results:

- $\sigma(a_1, ..., a_k)\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k))$ for $\sigma \in S_n$
- $(a_1, ..., a_k) = (a_1 a_k)(a_1 a_{k-1}) \ldots (a_1 a_2)$

cycle type of σ: $(n_1, \ldots, n_r)$, or $n_1 + \ldots + n_r$.

Prop. Two elements in S_n are conjugate to each other $\iff$ they have the same cycle type.

signature function of S_n: $sgn : S_n \xrightarrow{T} GL_n(\mathbb{R}) \xrightarrow{\det} \{\pm 1\}$, a surjective homomorphism.

$sgn(\sigma) = +1$ — even permutation. $sgn(\sigma) = -1$ — odd permutation.

Prop. If $\sigma = (a_1 ... a_k)$ is a k-cycle, then $sgn(\sigma) = (-1)^{k-1}$.

alternating subgroup of n elements: $A_n = \ker(sgn) = \{\sigma \in S_n | sgn(\sigma) = +1\}$, normal subgroup of S_n, consists of all the even permutations.

A group G is simple if it has no proper normal subgroups.