Logistics: Midterm I will be Thursday February 8 from 2:00-3:30 for in-person students. For remote students, it will be on either Thursday February 8 or Friday February 9. No notes, books or other aids.

Reminders:

1. Know the **formal definition**. Intuitive definitions are important for understanding but proofs require the use of the formal definition. If you are unsure of the formal definition, ask; don't guess.
2. All proofs should be formal and adhere to the same expectations as your written homework including the use of complete sentences, a clear beginning and conclusion, and appropriate use of symbols.
3. Unless explicitly stated otherwise, all answers require a rigorous explanation.
4. The emphasis will be on Chapters 3,4 and 5.

Topics:

Chapter 1

Definitions: equivalence relations, equivalence classes, set operations (intersections, unions, difference, Cartesian product, relations, functions, domain, range, image, one-to-one/injective, onto/surjective, bijective

Chapter 2

Definitions: greatest common divisor, least common multiple, relatively prime, Euclidean algorithm, prime number, composite number

Notation: $gcd(m,n)$

Results:

- Proof by mathematical induction.
- (Thm 2.9 The Division Algorithm) For every $a,b \in \mathbb{Z}$ such that $b > 0$ there exist unique $q,r \in \mathbb{Z}$, such that $a = qb + r$ where $0 \leq r < b$.
- (Lemma 2.13) Suppose $a,b \in \mathbb{Z}$ and p is a prime. If $p \mid ab$ then $p \mid a$ ore $p \mid b$.
- (Thm 2.15) The prime factorization of an integer is unique up to the order of the primes.

Chapter 3

Definitions: binary operation, associativity, identity, inverse, commutativity, group, order of a group, group of symmetries of an object, addition and multiplication modulo n, group of units, general linear group, subgroup, proper subgroup, trivial subgroup

Notation: $(\mathbb{Z},+)$ and with $\mathbb{R},\mathbb{Q}$, $(\mathbb{Z}_n,+)$, $(U(n),\cdot)$, $GL_n(\mathbb{R})$, $|G|$, $SL_2(\mathbb{R})$

Results:

- If G is a group, then
  - (Prop 3.17) the identity is unique.
  - (Prop 3.18) $\forall a \in G$, a^{-1} is unique.
  - (Props 3.19 and 3.20) $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$.
  - (Prop 3.21) $\forall a, b \in G$, equation $ax = b$ and $xa = b$ have unique solutions.
  - (Prop 3.22) $\forall a, b \in G$, both equations $ab = ac$ and $ba = ca$ imply $b = c$.
- (Thm 3.23) We can use the usual laws of exponents when manipulating repeated group operations on a single element. Specifically, if $g, h \in G$ a group and $m, n \in \mathbb{Z}$, then
  - $g^m g^n = g^{m+n}$
  - $(g^m)^n = g^{mn}$
  - $(gh)^n = ((gh)^{-1})^{-n} = (h^{-1}g^{-1})^{-n}$
- H is a subgroup of G if and only if
  - (Prop 3.30) (i) $e \in H$, (ii) $h_1h_2 \in H$ for every $h_1, h_2 \in H$, and (iii) $h^{-1} \in H$ for every $h \in H$.
  - (Prop 3.31) (i) $H \neq \emptyset$ and (ii)$gh^{-1} \in H$ for every $g, h \in H$.

Chapter 4

Definitions: Cyclic group, cyclic subgroup, generator of a group, cyclic subgroup generated by a, order of an element of a group,

Notation: $\langle a \rangle$, $|b|$, $n\mathbb{Z}$

Results:

- (Thm 4.9) Cyclic groups are abelian.
- (Thm 4.10) Every subgroup of a cyclic group is cyclic.
- (Prop 4.12) If $G = \langle a \rangle$ of order n, then $a^k = e$ if and only of $n \mid k$.
- (Thm 4.13) If $G = \langle a \rangle$ of order n and $b = a^\ell \in G$, then $|b| = \frac{n}{d}$ where $d = gcd(n, \ell)$.
- (Cor 4.11 of Prop 4.12) The subgroups of $(\mathbb{Z}, +)$ are $\langle 1 \rangle = \mathbb{Z}$, $\langle 2 \rangle = 2\mathbb{Z}$, $\langle 3 \rangle = 3\mathbb{Z}, \cdots$.
- (Cor 4.14 of Thm 4.13) Suppose $1 \leq r < n$. Then, $\mathbb{Z}_n = \langle r \rangle$ if and only if $gcd(n, r)$.

Chapter 5 Section 1

Definitions permutation, the symmetric group on n letters, a permutation group, disjoint cycles, transposition, even/odd permutation, length of a permutation.

Notation: S_X, S_n, permutation notation including disjoint cycle notation and transposition representation,

Results

- (Thm 5.1)The set of all permutations of the set X under function composition is a group.
- (Prop 5.8) Disjoint cycles permute.
- (Thm 5.9) Every permutation can be written as a product of disjoint cycles.
- (Prop 5.12) Any permutation of a finite set can be written as a product of transpositions, provided the set has at least two elements.
- (Thm 5.15) For every permutation σ, the parity (even or odd) of the number of transpositions in any transposition representation of σ is fixed. (i.e. always even or always odd).