

Preliminary:

1. Operations on Sets: Unions, Intersections, Complements, Set difference, Symmetric difference, Cartesian Product of sets, The power set, subsets, proper subsets, the empty set.
2. Properties of Integers: Division Algorithm, GCD, primeness, relative primeness, Euclidean Algorithm (to find the GCD of two integers), Theorem 4.2, Fundamental Theorem of Arithmetic.
 - Euclid's theorem about relatively prime integers (Theorem 4.3)
 - Two equivalent ways to define primeness
3. Well-Ordering Principle, Mathematical Induction (both forms)
4. Functions (Mappings): composite functions, one-to-one (= injective) functions, onto (= surjective) functions, bijective functions, invertible functions, image and pre-image of sets under a function
5. Complex Numbers: Arithmetic of complex numbers (addition, multiplication, division), Norms, Conjugates, Polar form of a complex number, roots of unity, the set U_n , the set $\mathcal{U}(1)$.

Binary Operations and Groups:

1. Binary Operations: Generalities, associativity, commutativity
2. Semigroup, Monoid, Group
 - Abelian Group, Order of a Group, Caley table for a group, the identity element of a group, inverse of an element in a group, Cancellation laws, Theorem 3.7 and Exercise 3.13, Exercise 3.7 (proved in class), Exercise 3.15 (proved in class) along with its corollary (converse to exercise 3.7 - proved in class)
3. Examples of Groups
 - \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , \mathbb{Q}^* , \mathbb{R}^* , \mathbb{C}^* , $\mathbb{Q}^+ = \{x \in \mathbb{Q} | x > 0\}$, $\mathbb{R}^+ = \{x \in \mathbb{R} | x > 0\}$
 - \mathbb{Z}_n , $m\mathbb{Z}$, \mathbb{Z}_p^* (p a prime), $U(n)$ and the Euler φ -function
 - \mathcal{U}_n , the circle group $\mathcal{U}(1)$ (also called the unitary subgroup of \mathbb{C}^*), $(\mathcal{P}(X), \Delta)$
 - \mathbb{R}^n , $M_n(\mathbb{R})$, general linear groups $GL_n(\mathbb{R})$ or $GL_n(\mathbb{Z}_p)$, the special linear group $SL_n(\mathbb{R})$,
 - $\mathbb{R}[x]$ along with $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_n[x]$
 - X^X , S_X (in particular $S_{\{1,2\}}$, $S_{\{1,2,3\}}$)
 - the group of unit quaternions Q_8 , the Klein 4-group V , $\mathbb{Z}_2 \times \mathbb{Z}_2$
4. Isomorphic groups, examples of isomorphic groups
 - $\mathbb{Z}_2 \cong U(4) \cong \mathcal{U}_2$
 - $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$
 - $\mathbb{Z}_n \cong \mathcal{U}_n$
 - Q_8 has three cyclic subgroups isomorphic to \mathcal{U}_4
 - ...

Subgroups:

1. Subgroup, proper nontrivial subgroup, lattice of subgroups
2. How to show a subset is a subgroup

Using the definition,

Thm: $\phi \neq H \subseteq G$ where G is a group. Then $H \leq G \Leftrightarrow \forall x, y \in H, xy^{-1} \in H$.

Theorem 5.3

3. Particular recipes to get subgroups: Given $a \in G, \langle a \rangle \leq G$; the center $Z(G) \leq G$.

Cyclic groups and subgroups:

1. $x^0, x^n, n \in \mathbb{Z}, \langle x \rangle$ if $x \in G$, additive & multiplicative notation for cyclic groups
2. Generator(s) of a subgroup
3. The order of an element $o(x)$, Facts about the order of an element (e.g. $o(x) = o(x^{-1}), o(x^k) = \dots$, i.e. Theorem 4.4)
4. The Fundamental Theorem of Cyclic Groups
 - Every subgroup of a cyclic group is cyclic
 - If $|\langle x \rangle| = n$, then the order of any subgroup of $\langle x \rangle$ is a divisor of n .
 - For each divisor k of $n = o(x)$, $\langle x \rangle$ has exactly one subgroup of order k , namely $\langle x^{\frac{n}{k}} \rangle$.
 - $\langle x^r \rangle = \langle x^s \rangle$ inside $\langle x \rangle$, a cyclic group of order n iff $(r, n) = (s, n)$.
5. The Fundamental Theorem of Cyclic Groups (as written in 4 above) is a reformulation of theorem 5.5 in the text.

Direct Products:

1. $G \times H, G_1 \times G_2 \times \dots \times G_n$
2. Theorem 6.1; Given finite cyclic groups $G_i, i = 1 \dots n$, when is $G = G_1 \times G_2 \times \dots \times G_n$ a finite cyclic group?
3. The Chinese Remainder Theorem (exercise 6.14 proved in class)
4. The Fundamental Theorem of Finite Abelian Groups

Every finite abelian group is isomorphic to a direct product of cyclic groups of prime-power order. Moreover the “factorization” is unique up to a rearrangement of the factors.

i.e., Every finite abelian group G is isomorphic to

$$\mathbb{Z}_{p_1}^{n_1} \times \mathbb{Z}_{p_2}^{n_2} \times \dots \times \mathbb{Z}_{p_k}^{n_k}$$

where the primes p_i are not necessarily distinct and the prime-powers $p_1^{n_1}, \dots, p_k^{n_k}$ are determined by G .