Definitions

Group: a set G endowed with an operation $* : G \times G \to G$ that has the following properties.

- well-defined: $a * b \in G$ for all $a, b \in G$;
- associativity: $a * (b * c) = (a * b) * c$
- unit: there exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$;
- inverses: for every $a \in G$ there exists an element $b \in G$ such that $a * b = b * a = e$ (denoted $b = a^{-1}$).

Abelian (commutative) group: a group $(G, *)$ with the property that $a * b = b * a$ for all $a, b \in G$.

Subgroup of a group $(G, *)$: a subset $H \subset G$ such that $(H, *)$ is a group (same operation as G).

Cyclic subgroup generated by an element a : $\langle a \rangle = \{a^n ; n \in \mathbb{Z}\}$. This is the smallest subgroup that contains a.

Cyclic group: A group that is generated by just one of its elements.

Order of a group: the number of elements in that group. Notation: $|G|$.

Order of an element: the number of elements in the subgroup generated by that element;

$$|a| = |\langle a \rangle| = \begin{cases} \min\{n \geq 1; a^n = e\} & \text{if such a power exists;} \\ \infty & \text{otherwise (i.e. } a^n \neq e \text{ for all } n \geq 1) \end{cases}$$

Centralizer of an element a**:** $C(a) = \{b \in G; a * b = b * a\}$ (it is subgroup of G).

Center of a group G**:** $Z(G) = \{b \in G; b * x = x * b \text{ for all } x \in G\}$ (it is a *normal* subgroup of G).

Cycle of length k**:** $(a_1 \dots a_k)$ is the permutation in S_n that takes $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, $\dots a_k \mapsto a_1$ and leaves all other numbers in $\{1, \dots, n\}$ alone.

Transposition: a $2-$cycle (ij) in S_n.

Even permutation: a permutation that is the product of an even number of $2-$cycles.

Odd permutation: a permutation that is the product of an odd number of $2-$cycles.

Group homomorphism: a map between two groups $f : (G_1, *) \to (G_2, \diamond)$ that is

- well-defined: $a_1 = b_1$ in $G_1 \implies f(a_1) = f(b_1)$ in G_2.
- operation-preserving: $f(a_1 * b_1) = f(a_1) \diamond f(b_1)$.

Isomorphism of groups: a bijective group isomorphism; i.e. a map between two groups $f : (G_1, *) \to (G_2, \diamond)$ that is

- well-defined: $a_1 = b_1$ in $G_1 \implies f(a_1) = f(b_1)$ in G_2.
- operation-preserving: $f(a_1 * b_1) = f(a_1) \diamond f(b_1)$ for all $a_1, b_1 \in G_1$.
- one-to-one (injective): $f(a_1) = f(b_1) \implies a_1 = b_1$.
- onto (surjective): for every $a_2 \in G_2$ there exists an element $a_1 \in G_1$ such that $f(a_1) = a_2$.

Isomorphic groups: two groups G_1 and G_2 are isomorphic if it exists an isomorphism $f : G_1 \to G_2$. Notation: $G_1 \cong G_2$ or $G_1 \approxeq G_2$ or $G_1 \approx G_2$ or $G_1 \backsimeq G_2$.

Automorphism of a group G: an isomorphism $f : G \to G$.

Inner automorphism of G induced by an element $a \in G$: $\phi_a : G \to G, \quad \phi_a(x) = axa^{-1}$.

External direct product of the groups $G_1, G_2, \dots, G_n$ is the group $G_1 \oplus \dots \oplus G_n = \{(g_1, \dots, g_n); g_1 \in G_1, \dots, g_n \in G_n\}$ with the operation performed componentwise.

Cosets: if H is a subgroup of G and a an element of G, the left coset of H containing a is $aH = \{ah; h \in H\}$ and the right coset of H containing a is $Ha = \{ha; h \in H\}$. In this case, a is called the coset representative of aH or Ha.

Index of a subgroup $H \subseteq G$ is the number of distinct left cosets of H. It is denoted by $|G : H|$. (it is also equal to the number of distinct right cosets of H).

Normal subgroup: a subgroup H of the group G for which the left and right cosets coincide, i.e. $aH = Ha$ for all $a \in G$ ($\Leftrightarrow aHa^{-1} = H$ for all $a \in G$). Notation: $H \lhd G$.

Factor group: if $H \lhd G$, the factor (quotient) group of G by H is $G/H = \{aH; a \in G\}$ the set of left cosets of H in G under the operation $(aH)(bH) = (ab)H$. We can also say G modulo (mod) H.

Internal direct product: A group G is the internal direct product of $H_1, H_2, \dots, H_m$ if all the H_i's are *normal* subgroups of G, $G = H_1 H_2 \dots H_m$, abd $(H_1 H_2 \dots H_i) \cap H_{i+1} = \{e\}$ for all $1 \le i \le m-1$. Notation: $G = H_1 \times H_2 \times \dots \times H_m$.

Kernel of a group homomorphism $f : G_1 \to G_2$ is $\ker f = \{a_1 \in G_1; f(a_1) = e_{G_2}\}$ (subset of G_1).

Image of a group homomorphism $f : G_1 \to G_2$ is $\operatorname{Im} f = \{f(a_1); a_1 \in G_1\}$ (subset of G_2).

Isomorphism class: to determine the isomorphism class of a finite abelian group G means to find a group of the form $Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}} \oplus \dots \oplus Z_{p_k^{n_k}}$ which is isomorphic to G. (Note: the primes $p_1, \dots, p_k$ do NOT have to be distinct.)

Greedy algorithm for an abelian group G of order p^n

1. Compute the orders of the elements of G.
2. Select an element a_1 of maximum order in G; set $G_1 = \langle a_1 \rangle$ and $i = 1$.
3. If $|G| = |G_1|$, STOP; if not, replace i by $i + 1$.
4. Select an element a_i of maximum order p^k such that $p^k \le \frac{|G|}{|G_{i-1}|}$ and none of the $a_i, a_i^p, \dots, a_i^{p^{k-1}}$ is in G_{i-1}; set $G_i = G_{i-1} \times \langle a_i \rangle$.
5. Return to step 3.

Theorems

1. Subgroup tests for a nonempty subset H of a group $(G, *)$

   One-step test: $a, b \in H \implies a * b^{-1} \in H$

   Two-step test: $a, b \in H \implies a * b \in H$ and $a \in H \implies a^{-1} \in H$

2. If $|a| < \infty$, then $|a^k| = \dfrac{|a|}{\gcd(k, |a|)}$.

3. If $|a| = \infty$ and $k \neq 0$, then $|a^k| = \infty$.

4. Every cyclic group is abelian. Therefore if a group is not abelian, it cannot possibly be cyclic.

5. However, even a nonabelian group has cyclic subgroups, and it can have other abelian subgroups. For instance, the center of G is an abelian subgroup of G.

6. An element a generates a *finite* group $G \Leftrightarrow |a| = |G|$.

7. The structure of a cyclic group $G = \langle a \rangle$ of order n

   - every subgroup of G is cyclic
   - the order of every subgroup divides $|G|$
   - the order of every element of G divides the order of the group
   - for every divisor d of n there exists a *unique* subgroup H of G with $|H| = d$; namely H is the cyclic subgroup generated by $a^{n/d}$
   - for every divisor d of n (including n), there are exactly $\varphi(d)$ elements of order d
   - if $k \nmid n$, there are no elements in G of order k

8. Permutations.

   - Disjoint cycles commute.
   - The order of a cycle is equal to its length.
   - Every permutation can be written *uniquely* as a product of disjoint cycles. Its order is the lowest common multiple of the lengths of those cycles.
   - Every permutation can be written as a product of transpositions.
   - Each permutations is either even or odd.
   - A cycle of odd length is even.
   - A cycle of even length is odd.
   - (even)$\cdot$(even)=even, (odd)$\cdot$(odd)=even, (even)$\cdot$(odd)=odd.

9. Properties of an isomorphism $f : G_1 \to G_2$

   - f^{-1} is an isomorphism.
   - $f(e_{G_1}) = e_{G_2}$.
   - $f(a^{-1}) = f(a)^{-1}$ for all $a \in G_1$.
   - $f(a^n) = f(a)^n$ for all $a \in G_1$ and all $n \in \mathbb{Z}$.
   - $ab = ba \Leftrightarrow f(a)f(b) = f(b)f(a)$.
   - G_1 is abelian if and only if G_2 is abelian.
   - $G_1 = \langle a \rangle \Leftrightarrow G_2 = \langle f(a) \rangle$. So G_1 is cyclic if and only if G_2 is cyclic.
   - $|f(a)| = |a|$.
   - $|G_1| = |G_2|$.
   - If G_1 is finite, then G_1 and G_2 have exactly the same number of elements of each order.
   - The equation $x^k = b$ has the same number of solutions in G_1 as does the equation $y^k = f(b)$ in G_2.
   - If H_1 is a subgroup of G_1, then $f(H_1)$ is a subgroup of G_2.

10. For every element $a \in G$, the map $\phi_a : G \to G$, $\phi_a(x) = axa^{-1}$ is an isomorphism.

11. G is abelian if and only if $\operatorname{Inn} G = \{\mathrm{Id}_G\}$.

12. $\operatorname{Aut}(Z_n) \approx U(n)$.

13. Properties of external direct products.
    - $G_1 \oplus \ldots \oplus G_n$ is abelian if and only if each G_i is abelian.
    - $|(g_1, \ldots, g_n)| = \text{lcm}(|g_1|, \ldots, |g_n|)$ in $G_1 \oplus \ldots \oplus G_n$.
    - If $G_1, \ldots, G_n$ are finite cyclic groups, then $G_1 \oplus \ldots \oplus G_n$ is cyclic if and only if $\gcd(|G_i|, |G_j|) = 1$ for all $i \neq j$.
    - $Z_{n_1 n_2 \ldots n_k} \approx Z_{n_1} \oplus \ldots \oplus Z_{n_k}$ if and only if $\gcd(n_i, n_j) = 1$ when $i \neq j$.
    - If $\gcd(n_i, n_j) = 1$ when $i \neq j$, then $U(n_1 \ldots n_k) = U(n_1) \oplus \ldots \oplus U(n_k)$.
    - $U(p^n) \approx Z_{p^n - p^{n-1}}$ for a prime $p > 2$.
14. Properties of cosets (H is a subgroup of G, $a, b \in G$)
    - $a \in aH$
    - $b \in aH \implies bH = aH$
    - $a, b \in G \implies$ either $aH = bH$ or $aH \cap bH = \emptyset$
    - $aH = bH \Leftrightarrow a^{-1}b \in H \Leftrightarrow b^{-1}a \in H$
    - $Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow ba^{-1} \in H$
    - aH is a subgroup $\Leftrightarrow aH = H \Leftrightarrow a \in H$
    - $|aH| = |Ha| = |H|$
    - $aH = Ha \Leftrightarrow aHa^{-1} = H$
15. Lagrange's Theorem
    If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$ and $|G : H| = \frac{|G|}{|H|}$.
16. Consequences of Lagrange's Theorem.
    - The order of every element a of a group G divides the order of G.
    - For all $a \in G$, $a^{|G|} = e$.
    - If G is a group of order p and p is a prime, then G is cyclic (and therefore isomorphic to Z_p).
17. **Normal subgroup test** for a subgroup H of G : $aha^{-1} \in H$ for all $h \in H$ and $a \in G$.
18. G/H is a group under left coset multiplication $(aH)(bH) = (ab)H$. The unit is the coset $eH = H$ and inverses are given by $(aH)^{-1} = (a^{-1})H$.
19. Cauchy's Theorem for abelian groups
    If G is a finite abelian group of order n and p is a prime that divides n, then G contains an element of order p.
20. If a group G is internal direct product $G = H_1 \times H_2 \times \ldots \times H_m$ of a finite number of (normal) subgroups, then G is isomorphic to the external direct product $H_1 \oplus H_2 \oplus \ldots \oplus H_m$ of those subgroups.
21. Properties of homomorphisms: let $f : G_1 \to G_2$ be a group homomorphism. Then
    - $f(e_{G_1}) = e_{G_2}$.
    - $f(a^{-1}) = f(a)^{-1}$ for all $a \in G_1$.
    - $f(a^n) = f(a)^n$ for all $a \in G_1$ and all $n \in \mathbb{Z}$.
    - $ab = ba \implies f(a)f(b) = f(b)f(a)$.
    - If $|a|$ is finite, then$|f(a)|$ divides $|a|$.

- If $f(a) = b$, then $f^{-1}(b) \overset{\text{definition}}{=} \{x \in G_1; f(x) = b\}$ is equal to the left coset $a \ker f$.
- If H_1 is a subgroup of G_1, then $f(H_1) \overset{\text{definition}}{=} \{f(x); x \in H_1\}$ is a subgroup of G_2. In particular, $\operatorname{Im} f$ is a subgroup of G_2.
- If H_2 is a subgroup of G_2, then $f^{-1}(H_2) \overset{\text{definition}}{=} \{x \in G_1; f(x) \in H_2\}$ is a subgroup of G_1.
- If K is a normal subgroup of G_2, then $f^{-1}(K)$ is a normal subgroup of G_1. In particular $\ker f$ is a normal subgroup of G_1.
- f is injective $\Leftrightarrow \ker f = \{e_{G_1}\}$.

22. First Isomorphism Theorem
If $f : G_1 \to G_2$ is a group homomorphism, then $F : G_1/\ker f \to \operatorname{Im} f$, $F(x \ker f) = f(x)$ is an isomorphism.

23. If G_1, G_2 are finite groups and $f : G_1 \to G_2$ is a group homomorphism, then $|\operatorname{Im} f|$ divides both $|G_1|$ and $|G_2|$. So it divides $\gcd(|G_1|, |G_2|)$.

24. Every normal subgroup H of G is the kernel of a group homomorphism. Namely, it is the kernel of the natural mapping $f : G \to G/H$, $f(x) = xH$.

25. Chinese Remainder Theorem
If m, n are two positive integers and $\gcd(m, n) = 1$ then for any $a, b \in \mathbb{Z}$ there exists an integer x such that $x \equiv a \pmod m$ and $x \equiv b \pmod n$.

26. Fundamental theorem of finite abelian groups
Every finite abelian group G is isomorphic to a group of the form $Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}} \oplus \ldots \oplus Z_{p_k^{n_k}}$. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by G.

27. If G is a finite group of order n and $m|n$, then G has (at least) a subgroup of order m.

Examples of groups

1. $\mathbb{Q}, \mathbb{R}$ are groups under addition. $\mathbb{R}^*, \mathbb{Q}^*, \mathbb{R}^*_+, \mathbb{Q}^*_+$ are groups under multiplication.

2. $\mathbb{Z}$ is a group with $+$. It is the quintessential example of an infinite cyclic group.
   - generated by 1 and -1; that is, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$
   - all its subgroups are cyclic, generated by nonnegative integers; they are of the form $\langle n \rangle = n\mathbb{Z}$
   - $m \in \langle n \rangle \Leftrightarrow m$ is a multiple of n

3. Z_n is group under addition modulo n. It is the quintessential example of a cyclic group of order n.
   - generated by 1
   - it is in fact generated by all k with $\gcd(k, n) = 1$; these are all its generators
   - its subgroups are of the form $\langle d \rangle$ where $d|n$; and $|\langle d \rangle| = |d| = n/d$.
   - it has $\varphi(d)$ elements of order $d|n$ and no elements of any order that does not divide n
   - the one and only subgroup of order $d|n$ of G has exactly $\varphi(d)$ generators, namely the elements of G of order d

4. $U(n) = \{1 \le k \le n; \gcd(k, n) = 1\}$ is a group under multiplication modulo n.
   - It has order $\varphi(n) = \varphi(p_1^{c_1})\varphi(p_2^{c_2}) \ldots \varphi(p_r^{c_r})$, if $n = p_1^{c_1} \ldots p_r^{c_r}$.
   - Recall that φ is called Euler's phi function and that $\varphi(p^c) = p^{c-1}(p-1)$.

- The group $U(n)$ is abelian, but not necessarily cyclic. (E.g. $U(8)$ is not cyclic.)
- It is NOT a subgroup of Z_n since they don't have the same operation.

5. D_n is the group of symmetries of the regular n-sided polygon.

   - Its elements are transformations of the 2-dimensional real plane into itself that leave the polygon in the same position in the plane. So they are function $\mathbb{R}^2 \to \mathbb{R}^2$ that preserve a regular n-sided polygon centered at the origin.
   - It has $2n$ elements: n rotations ($R_0, R_{2\pi/n}, \ldots, R_{2(n-1)\pi/n}$) and n flips across the symmetry axes of the polygon.
   - It is not abelian.
   - Rotation $\circ$ flip = (another) flip, flip $\circ$ rotation = (yet another) flip, flip $\circ$ flip = rotation
   - The elements of D_n can be expressed as 2×2 real matrices.

6. $\mathrm{GL}(2, F)$ the group of 2×2 *invertible* matrices with entries from $F = \mathbb{Q}, \mathbb{R}, \mathbb{Z}$ or Z_p (p is a prime). This is a group under matrix multiplication (all arithmetic is done in F, so modulo p in case of Z_p).

   - Saying that a matrix is invertible is the same as saying that its determinant has an inverse in F. That means the determinant is $\neq 0$ if $F = \mathbb{Q}, \mathbb{R}, Z_p$. But when $F = \mathbb{Z}$ this amounts to the determinant being ± 1.
   - It is not abelian.
   - Its center is $\{\lambda I; \lambda \in F\}$, where $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

7. $\mathrm{SL}(2, F)$ is the group of 2×2 matrices with entries from $F = \mathbb{Q}, \mathbb{R}, \mathbb{Z}$ or Z_p (p is a prime) and determinant 1. This is a group under matrix multiplication (all arithmetic is done in F, so modulo p in case of Z_p).

   - It is not abelian.
   - It is a normal subgroup of $\mathrm{GL}(2, F)$.

8. S_n the group of permutations of n objects. This is a group under composition.

   - It has $n!$ elements. Half of them are odd permutations and half of them are even permutations.
   - It is not abelian.

9. A_n the alternating group of order n is the group of *even* permutations of n objects. This is a group under composition.

   - It has $n!/2$ elements.
   - It is not abelian.
   - It is a normal subgroup of S_n.

10. $\mathrm{Aut}(G)$ is the group of automorphisms of the group G. It is a group under composition.

    - Its unit is Id_G the identity map.
    - In general it is not abelian.

11. $\mathrm{Inn}(G)$ is the group of inner automorphisms of the group G.

    - It is a subgroup of $\mathrm{Aut}\, G$.
    - In general it is not abelian.
    - It is isomorphic to $G/Z(G)$.