Chapter 1

Groups

Note to the reader: This is not an exhaustive list of important results required for competitive exams but rather a starting point. The git hub link for these notes is https://github.com/aaron12alphonso/
Notes.git

1.1 Basic Counting Results in Groups

Theorem 1.1.1. *If G is a group and $x \in G$ is of order n then for any $k \in \mathbb{N}$*

$$|x^k| = \frac{n}{\gcd(n,k)}$$

Theorem 1.1.2. *Let G be a group and $x \in G$ be of order n and suppose $s, t \in \mathbb{N}$. Then $\langle x^s \rangle = \langle x^t \rangle$ if and only if $\gcd(n,s) = \gcd(n,t)$.*

Theorem 1.1.3 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G then $|G| = |H||G/H|$ and hence $|H|$ divides $|G|$.*

Theorem 1.1.4. *If H and K are finite subsets of a group G then*

$$|HK| = \frac{|H||K|}{|H \cap K|} \tag{1.1.1}$$

Theorem 1.1.5 (Sylow's Theorem)**.** *Let G be a group of order $p^\alpha m$ where p is a prime such that $p \nmid m$ Then*

1. *G has a subgroup of order p^α i.e G has a Sylow $p-$ subgroup.*
2. *If P and Q are Sylow $p-$ subgroups then $Q = gPg^{-1}$ for some $g \in G$.*
3. *If n_p is the number of Sylow $p-$ subgroups of G then $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$.*

Theorem 1.1.6. *If p and q are primes such that $p < q$ and $q \not\equiv 1 \pmod{p}$ then and group of order pq is cyclic.*

Theorem 1.1.7 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *If G is a finitely generated abelian group then there exists integers $r, n_1, n_2, \ldots, n_s$ such that $|G| \equiv \mathbb{Z}^r \times$*

$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ *where*

1. $r \geqslant 0$ *and* $n_j \geqslant 0$ *for* $1 \leqslant j \leqslant s$
2. $n_{j+1} \mid n_j$ *for* $1 \leqslant j \leqslant s-1$

1.2 Homomorphisms

Theorem 1.2.1. *Let $f : G \to H$ be a group homomorphism. Then we have the following properties*

- *For any finite subgroup S of G, $|f(S)| \mid |S|$*
- *For any $a \in G$ of finite order $|f(a)| \mid |a|$*

Remark. Notice how the above theorem can help you to compute the number of homomorphisms from some group G to another group H.

1.3 The Group $\mathbb{Z}_n$

Theorem 1.3.1. *For $n \in \mathbb{N}$, $\mathbb{Z}_n$ has the following properties*

- *The group $\mathbb{Z}_n$ has exactly $\phi(n)$ generators.*
- *The number of subgroups of $\mathbb{Z}_n$ are the number of divisors of n.*
- *For $a \in \mathbb{Z}_n$, $|a| = \dfrac{n}{\gcd(a,n)}$*
- *For $a, b \in \mathbb{Z}_n$, $< a >=< b >$ if and only if $\gcd(a,n) = \gcd(a,n)$.*

Theorem 1.3.2. *The number of homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$ is $\gcd(n,m)$.*

1.4 The Group S_n

-The group of all permutations of an $n-$ set

Theorem 1.4.1 (Properties of S_n)**.**

1. *The set of all transpositions is a generating set of S_n*
2. *For $\sigma = (a_1, a_2, \ldots, a_k) \in S_n$ and $\tau \in S_n$, $\tau\sigma\tau^{-1} = (\tau(a_1), \tau(a_2), \ldots, \tau(a_k))$.*
3. *The for any $n-$ cycle σ and any transposition τ in S_n the set $\{\sigma, \tau\}$ generates S_n.*
4. *The number of conjugacy classes of S_n is the number of partitions of n, $p(n)$.*
5. *The order of a permutation in S_n is the lcm of the lengths of it's cycles when the permutation is written as a product of disjoint cycles.*

1.5 The Group D_{2n}/D_n

- The group of all symmetries of a regular polygon of $n-$ vertices.

Theorem 1.5.1 (Properties of D_n).

1. *D_{2n} consist of $2n$ elements, n of which are rotations and the rest are reflections*
2. *If s is the reflection of the regular $n-$ gon about the line of symmetry that passes through the vertex 1 and the origin and suppose r is the rotation of the regular $n-$ gon by $2\pi/n$ radians then $D_{2n} = \{sr^k : 0 \leqslant k \leqslant n-1\}$*
3. *The composition of two rotations is a rotation.*
4. *The composition of a rotations and a reflection is a reflection.*
5. *The composition of two reflections is a rotation.*
6. *The inverse of a rotation is a rotation.*
7. *The inverse of a reflection is the same reflection. That is reflections are order 2 elements of D_{2n}*

1.6 The Group A_n

- Subgroup of all even permutations of an $n-$ set

Theorem 1.6.1 (Properties of A_n).

$|A_n| = n!/2$ and hence A_n is a normal subgroup of S_n.

For any subgroup H of A_n either $H \subset A_n$ or $|H \cap A_n| = |H|/2$.

The set $\{(1,2,3),(1,2,4),\ldots,(1,2,n)\}$ is a generating set of A_n.