Math 110AH Reference Sheet

Nathan Solomon

December 14, 2023

Still need to write notes on the following:

- review Charlie's notes
- Sylow's theorems
- solvable, normalizer, derived series, dicyclic group (specail case with 8 elements is called the quaternion group), semidirect product (internal and external), construction of dihedral group as a semidirect product, isotropy group, effective action, nilpotent group, characteristic subgroup
- center of dihedral group. Cauchy's theorem

The **division theorem** says that for any integers a, b such that $b \neq 0$, there exist unique integers q and r (called the "quotient" and "remainder", respectively) such that $a = qb + r$ and $0 \leq r < |b|$.

Bézout's identity says that if $a, b, c, x_0, y_0 \in \mathbb{Z}$ and $d = \gcd(a, b)$ and $ax_0 + by_0 = c$, then the pair of integers (x, y) is a solution to $ax + by = c$ if and only if

$$(x, y) = \left(x_0 + \frac{bk}{d}, y_0 - \frac{ak}{d}\right)$$

for some integer k.

An **isomorphism** can be defined as a bijective homomorphism. This is not always true, but in the context of groups and the material we cover in this class, it works.

The **order of a group** G is just the cardinality $|G|$, but the **order of an element of a group** is the order of the subgroup generated by that one element. For example, the cyclic group of 4 elements (C_4) and the Klein 4-group (K_4) both have order 4, but one way to tell they're not isomorphic is to note that C_4 contains two elements of order 4, but in K_4, all elements except the identity have order 2.

Cauchy's theorem says that for any finite group G whose order is divisible by a prime number p, there must be an element $g \in G$ with order p.

The **Chinese remainder theorem** says that if $n_1, n_2, \ldots, n_k$ are pairwise coprime and $N = n_1 n_2 \cdots n_k$, then

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

In other words, if we know the remainder when some integer a is divided by n_1, when it's divided by n_2, and so on all the way to n_k, we know what the remainder is when a is divided by N.

Euler's totient function is a function $\varphi : \mathbb{N} \to \mathbb{N}$ defined as follows:

$$\varphi(n) = \left|\{k \in \mathbb{N} : k \leq n, \gcd(n,k) = 1\}\right|.$$

If $n \neq 1$ then $\varphi(n)$ is equal to the number of generators of the cyclic group of order n, and it's also equal to the order of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. Once you know the prime factors of n, you can calculate $\varphi(n)$ very quickly using the following rules, which come from the Chinese remainder theorem:

- If p is prime and $k \geq 1$, then $\varphi(p^k) = p^{k-1}(p-1)$.
- If a and b are coprime, then $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Euler's theorem says that if a and n are coprime positive integers, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Also, if that congruence is true for some positive integers a and n, then a and n are coprime.

Lagrange's theorem says that if H is a subgroup of a finite group G, then

$$|G| = [G : H] \cdot |H|.$$

Fermat's little theorem says that if p is prime and a is coprime to p, then

$$a^{p-1} \equiv 1 \pmod{p},$$

which is easy to get from Euler's theorem. But more generally, if p is prime and a is any integer, then Fermat's little theorem also says

$$a^p \equiv a \pmod{p}.$$

The **Euclidean algorithm** calculates the greatest common divisor of two natural numbers in logarithmic time. If you ever forget how it works, just picture that one gif from wikipedia where a rectangle is being tiled by squares.

If S is a subset (not necessarily a subgroup) of a group G, then the **free group** generated by S is written as $\langle S \rangle$ and is defined as the intersection of all subgroups of G which contain all the elements of S.

If H is a subgroup of G, then the **quotient**, $G/H := \{gH : g \in G\}$, is the set of all left cosets of H (in G). The quotient is a group if and only if $H \trianglelefteq G$ (H is normal in G).

The **first isomorphism theorem** says that if $f : G \to H$ is a group homomorphism, then $Ker(f)$ is normal in G, $Im(f)$ is a subgroup of G, and $Im(f) \cong G/Ker(f)$.

The **second isomorphism theorem** says that if S is a subgroup of G and N is a normal subgroup of G, then $(SN)/N \cong S(S \cap N)$.

The **third isomorphism theorem** says that if N and K are both normal subgroups of G and $N \subset K$, then $(G/N)/(K/N) \cong G/K$.

The **universal property of quotient groups** is that if G and H are groups, N is a normal subgroup of G, and $f : G \to H$ is a group homomorphism whose kernel conttains N, then there exists a unique group homomorphism $\overline{f} : G/N \to H$ such that $f = \overline{f} \circ \pi$, where π is the canonical homomorphism from G to G/N.

The **center** of a group G, written as $Z(G)$, is the set of elements which commute with all other elements of G.

An **inner automorphism on** G is an isomorphism from G to G that can be defined as conjugation by some element of G. The set of all inner automorphism of G is called $Inn(G)$, and by the first isomorphism theorem,

$$G/Z(G) \cong Inn(G).$$

The **outer morphism group** is defined as $Out(G) = Aut(G)/Inn(G)$.

The **conjugacy class** of an element $x \in G$ is the set of all elements of the form gxg^{-1} for some $g \in G$. One interesting example is the alternating group A_n when $n \geq 5$. We proved in class that when $n \geq 5$, A_n is **simple**, meaning it has no normal subgroups, so the conjugacy classes of A_n are IDK.

A **perfect** group is equal to its own commutator subgroup.

The **orbit-stabilizer theorem** says that if the group G acts on X, then for any $x \in X$, there is a bijection between $G/Stab(x)$ and $Orb(x)$, so $|G \cdot x| = |Orb(x)| = [G : Stab(x)] = [G : G_x] = |G|/|G_x|$.

A group action is **faithful** if the only element which behaves like the empty permutation is the identity element of the group. It is called **transitive** if there is only one orbit.

Here is a **list of all groups of order below 16**:

Order	Abelian groups	Non-Abelian groups
1	$C_1 \cong \{e\}$	
2	C_2	
3	C_3	
4	C_4, K_4	
5	C_5	
6	C_6	$D_3 \cong S_3$
7	C_7	
8	$C_8, C_2 \oplus C_4, C_2 \oplus C_2 \oplus C_2$	D_4, Dic_2
9	$C_9, C_3 \oplus C_3$	
10	C_{10}	D_5
11	C_{11}	
12	$C_{12}, C_2 \oplus C_6$	D_6, A_4, Dic_3
13	C_{13}	
14	C_{14}	D_7
15	C_{15}	
...	...	...