Part I

Revison lecture:

$\star$ Important idea's

1 Group:

a group is a set with an operation

$(G, *)$.a group has 3 conditons: (as well $*$ must be a Binary op. (it may be stated in the question that is is)

- * is ascociative
- There is an identity element
- every element has an inverse

2 Subgroup

A subgroup is a subset of your group, that is also a group under the same operation

2.1 1st/2nd subgroup test

First for either, must show group is nonempty. (often best to show it contains the identity)

2.1.1 1st subgroup test

$\forall a, b \in H \subseteq G$ shopw that $ab \in H$and $a^{-1} \in H$

2.1.2 2nd subgroup test

$\forall a, b \in H$,$ab^{-1} \in H$

3 Order of an element

The order of an element g is the minim number of time you must apply the operatution, to get he identity

ie the smallest positive intetger n, such that $g^n = e$. if no such uinteger exist then $g$has infinite order

3.0.3 Order of identity element:

is 1.

3.1 Order of powers of an elemnt

if $|g| = n$ then $|g^k| = \frac{n}{gcd(n,k)}$

3.1.1 Order of element divides order of group

by collary of lagrange: if G is finite, and $g \in G$then the order of g divideds $|G|$

3.1.2 Cauchy's theorem

if $G$is a finite group, and p is a prime dividing $|G|$ then G contains a element of order p.

4 Cylic groups

A group Gi s cyolcic if $G = \langle g \rangle$ for some $g \in G$

4.1 $\star$Every sybgroup of a cylic groups is cylcic

4.2 If G is a cyclic group of ordr n, and $r|n$ then G has a unique subgroup of order r

4.3 Isomorphic to $\mathbb{Z}$

Any infinite cyclic group is isomorphc to $\mathbb{Z}$

any finite cylcic group of order n is isomorphic to $\mathbb{Z}_n$

5 Permuation groups

S_n , $Sym(\Omega)$

5.1 Every permuations can be written as a product of transpostions

these don't have to be disjoint

Eg $(123) = (12)(13)$

5.1.1 $\star$ That product of transpositions ie either always even or always odd.

Though there may be many way of wriyting it as product of transpositions

5.2 $\star$Ruffins theorum

The order osa a permuation when written as a product of disjoine cylces is the lcm of the cycle lengths

5.3 NOT EXAMINABLE: Futurama theorem

let A be a finite set and let x, y be an extra 2 elements.

then for any permuations σ of A,

we can multiply σ by a product of disjoint transpositions each containing one of x,or y or both.

5.3.1 Proof:

for one a once cylce permuation of length k: $(123...k)(xk)(y, k-1)(y, k-2)...(y, 1)(x, k-1)(y, k) = (x, y)$ and then $(x, y)(x, y) = ()$

if we had 2 cycles $(123...k_1)(abc...k_2)$

6 Cosets

$H \leq G$, $g \in G$

$Hg = \{hg | h \in H\}$

- If G is finite them $|H| = |Hg|$
- cosets partition group
- $Ha = Hb \iff ab^{-1} \in H$
  - if $a \in H$ then $Ha = H$

6.0.2 Complete set of right coset repressitives for H is:

is a subset X of G, such that ever coset of H can be written as Hx for some $x \in X$

And for $x_1, x_2 \in X$: $Hx_1 \neq Hx_2$for $x_1 \neq x_2$

6.1 Normal subgroups

$H \lhd G$

$\iff Ha = aH$for all $a \in G$

$\iff a^{-1}Ha = H$ for all $a \in G$

$\iff a^{-1}Ha \subseteq H \ \forall a \in G$ (normal subgroup test

6.1.1 All subgorups of abeleian groups are normal.

7 Group actions

- orbits
  - written for element α: α^G
- stabalisers
  - written for element α: G_α

7.0.2 $\star$ Orbit stabaliser theorem

_let $G \leq Sym(\Omega)$with $|G|$finite. then
$|G| = |\alpha^G||G_\alpha|$ for $\alpha \in G$

8 Homomorphism:

$\phi : G \to H$is a hm, if $(ab)\phi = (a)\phi(b)\phi\ \forall a, b \in G$

8.0.3 Kernal:

ker $\phi = \{g \in G|(g)\phi = e_H\}$
$ker\, \phi \lhd G$

8.0.4 Onto

a homomorphism is onto one iff the kernal is trivial ($ker\, \phi = \{e_G\}$)

8.1 Isomorphism:

a one to one and onto hm.

8.2 Automoporphism

an automorphism aof a group G is a isomprhism $\phi : G \to G$
group of all automorphjisms of G is $Aut(G)$

8.2.1 inner auto

ι_g : G$\to$G is an autom
$x \mapsto g^{-1}xg$
$Inn(G) = \{\iota_g | g \in G\} \lhd Aut(G)$

8.2.2 $\star$Conjuugation in S_n

two elements of S_n are conjugate iff they hyave the same cycle structure

8.2.3 Conjugate Subgroups

let $H$and K be subgroups of G. then $H$is conjuage to Kif $\exists g \in GH = g^{-1}kg$

9 $\star$Legrange' Thm

LEt G be a finite group, and $H \leq G$.
Then $|H| \mid |G|$ (order of H divides the order of $|G|$)

9.0.4 Converse not always true

Let G be a group of order n. let $r|n$. You cannot gareentee there is a subgour of order r

Your can if:

- G is cylic.
- or G is abelain (Fundermental theroem of finte abeleian groups)
- or if r is a prime power (Sylows therom)

10 ⋆Fundermental theroenm of fintite abeleian groups

Let Gbea finte abelian group

then $G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times ..\mathbb{Z}_{p_r^{a_r}}$

for some primes mp_i and positive integers ma_i

moreover the cylcif factos m$\mathbb{Z}_{p_i^{a_i}}$ are unique up to ordering.

11 ⋆Slows therm

let G be a group of order $p^r m$ with pa rime, $r \in \mathbb{Z}_+$and $gcd(p, m) = 1$

- G has a subgroup of ordr p^r. Called a Sylow p-subgroup
- all sylow subgroups are conjugate.
- any p-subgoups of mG is containsed ina a sylow $p - subgroup$
- If n is the number of Sylow p-subgroups then $n \equiv (mod\, p)$ and $n \mid m$

11.1 if there is only one sylow p-subgroup is normal

a saylow $p - subgroup$is norma lin Giff the unique $Sylow, p - subgroup$

11.2 Interctrion (of groups of coprime order) is trival

is $|P| = 5^2$, $|Q| = 7$ then $P \cap Q \leq G$, and $P \cap Q \leq G$,, $P \cap Q \leq P$, $P \cap Q \leq Q$

thus $|P \cap Q \leq G| \mid |P$ and $|P \cap Q \leq G| \mid Q$

thus suince $gcd(|P|, |Q|) = 1$ $|P \cap Q \leq G| = 1$ so it just hte identity

12 Direct Product

external diret product: for H, K groups:

$H \times K = \{(h, k)|h \in H, k \in K\}$

12.0.1 ⋆Identifing something as the resuklt of a direct product

let Gbe a group with normal subgroups N_1, N_2, and $N_1 \cap N_2 = e$
and $G = N_1N_2 = \{n_1, n_2 | n_1 \in N_1, n_2 \in N_2\}$
then $G \cong N_1 \times N_2$

12.0.2 Groups of order p^2

are either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$

13 Quotient Groups

for G a group and $H \lhd G$ then G/H is the group of all right coset of H in G with the b. op:
$(Ha)(Hb) = H(ab)$

13.0.3 Corresponace theorem

$H \lhd G$,
$H \leq K \leq G$
then $K \cong G/H$

13.1 ⋆ 1st isomorphis theorem

let $\phi : G \to H$be a hm.
then $G/ker\,\phi \cong (G)\phi \leq H$

13.2 ⋆ Cayleys therom

Every group is isomorphic to a subgroup of $Sym(\Omega)$ for some set Ω.
As if
G acts on Ω then $\exists hm\, \phi : G \to Sym(\Omega)$

14 ⋆Orbit counting Lemma

15 Affine groups:

$AGL(n, F) = \{t_{A,v} | A \in GL(n, F) v \in F^n\}$
$t_{a,v} : F^n \to F^n : x \mapsto xA + v$
for any field