H2: Finite groups, basic definitions and properties

2.1 basic definitions, examples, Cayley table	
def: finite group G	= a finite set of elements $\{g_i\}$ wich transforms into each other associatively by a multipl. law: $\cdot : G \times G \to G$ > must have: - identity element 1, such that: $g \cdot 1 = 1 \cdot g = g$ - every g has a unique inverse: g^{-1}: $g \cdot g^{-1} = 1 = g^{-1} \cdot g$.
order/cardinality of a group	= number of group elements > #G or $\|G\|$
order n of a group element g	= smallest power n>=1 one has to take such that it's equal to the identity element: $g^n = 1$
Abelian group	= group for which the mult. is commutative
representation of a group	= defining a group through a generating set of group elements > ie a minimal set of group elements whose multiplication with each other, whose products generate the whole group
2.1.1 first examples	
cyclic group Z_n	= group of integers {0,1,…,n-1} with multiplication addition modulo n > we can think of it as the cyclic permutation of n letters
permutation group S_n	= group of n elements with multipl. the composition of permutations > write the permutations $\sigma \in S_n$ as: $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$ For example: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} \in S_6$ > its possible to write permutations as a collection of disjoint cycles > ie: sets of elements that are cyclically permutated >> in our example: (124)(35)(6) > cycle notation is unique up to cyclic permutations within each cycle: (124)(35) = (53)(241) >> $\|S_n\| = n!$
dihedral group D_n	= group of symmetries of a regular n-gon > n cyclic rotations and n reflections through n axes > $D_n = Z_n \rtimes Z_2$ >> $\|D_n\| = 2n$
group representation of Z_n	$\mathbb{Z}_n = \langle a \| a^n = 1 \rangle$ according to the specific mult. rule
2.1.2 Cayley table	
Cayley table	= shows how the group multipl. behaves > ie the entry (g,h) denotes the element g.h: *For the cyclic group Z_2 we have* $C = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
2.1.3 direct products	
def: direct product × or ⊕	For two groups G and H > the direct product G×H is a group with elements that can be labelled by the set of tuples (g_i, h_i) for which $(g_i,h_j) . (g_k,h_l) := (g_i.g_k, h_j.h_l)$ now also: $\|G \times H\| = \|G\|\|H\|$

2.2 homomorphisms, isomorphisms and automorphisms	
def: map	for two groups G_1 and G_2 > we can devise maps between these groups by mapping the elements of G_1 to G_2 > there is no guarantee that such a map will preserve the multipl. law
def: homomorphism	= map φ: $G_1 \rightarrow G_2$ for which $\varphi(xy) = \varphi x)\varphi(y)$, ie preserves multipl. law > we thus have: $\varphi(g^{-1}) = \varphi(g)^{-1}$ and $\varphi(1_{G1}) = 1_{G2}$
prop: image of a hom. is a group	The image of a homomorphism φ: $G_1 \rightarrow G_2$ is a subgroup of its codomain G_2: $\varphi(G_1) \leq G_2$
def: isomorphic groups	= there exists a bijective homomorphism φ: $G_1 \rightarrow G_2$ between G_1 and G_2 > φ is an isomorphism of groups > $G_1 \cong G_2$
def: automorphism	= an isomorphism from G to itself
def: automorphism group Aut(G)	= group of all automorphisms of G with group mult. the composition of maps
def: inner automorphisms Inn(G)	= automorphisms of G obtained by relabelling using conjugation with respect to a fixed group element : g_i: $g_j \rightarrow g_i g_j g_i^{-1}$
def: U(1)	U(1) = $\{z \in \mathbb{C} \mid \lvert z \rvert^2=1\}$ with group mult. the mult. of complex numbers > is an Abelian group with trivial inner automorphisms > automorphisms can be labelled by functions f(x) that have to satisfy: $$\forall x, y : f(x+y) = f(x) + f(y) \mod 2\pi$$ and in particular: $$f(x) + f(2\pi - x) = 2\pi n \text{ with } n \text{ an integer.}$$ > these conditions imply f(x) = nx > can only be an isomorphism for n=+-1 > the automorphism group of U(1) is Z_2, the reflection group
2.3 subgroups, cosets, normal subgroups, quotient groups	
def: subgroup S of a group G	= a subset of elements of G such that they form a group themselves with the group mult. that of G restricted to S > S≤G or S<G if S!=G
trivial vs proper subgroups	A group always has two *trivial* subgroups: the trivial group and itself > all other subgroups are *proper* subgroups
finding subgroups via Cayley	To find a subgroup is to find a submatrix in the Cayley table of G which is a Cayley table itself
def: left coset	For a subgroup H≤G > the left coset of H in G are the sets $gH:=\{gh \mid h \in H\}$ Note that $g_1 \sim g_2$ <=> $g_1H = g_2H$ or thus $g_1 g_2^{-1} \in H$ defines an equivalence relation > the cosets are exactly the equivalence classes
G/H	= collection of all (left) cosets of H in G > isn't necessarily a group
index of H in G	= |G/H|
th: Lagrange's theorem	For H a subgroup of G, H≤G > then the elements of G/H are disjoint subsets of G whose union is G and each coset has the same number of elements #H, hence #H divides #G
prop: subgroups of Z_p	Z_p with p a prime number has only trivial subgroups
prop: order of finite group	The order of every group element of a finite group divides the order of the group
centre Z(G) of a group G	= subgroup whose elements commute with all elements of G > can be found by searching for zero rows in the matrix $C-C^t$
def: conjugacy class	= for a group element g∈G this is $C_g:=\{hgh^{-1} \mid h \in G\}$ > we can partition the group in different classes, where every element is contained in exactly one class > - order of alle elements in a class is constant - the representative g is not unique, thus belonging to the same class is a equiv. relation

def: normal subgroup	For a subgroup N≤G > N is normal if its invariant under conjugation with all group elements of the group G > then Ng = gN for all g∈G ie: if you conjugate any element of N with any of G, you again get an element of N notation: N ⊴ G
simple group	= group for which its only normal subgroup is the trivial group
def: quotient group	For a group G with normal subgroup N⊴G > define G/N as the group with elements the cosets gN and group mult.: $g_1N \cdot g_2N := (g_1g_2)N$ > we then have |G/N|=|G|/|N|
maximal normal subgroup	= normal subgroup for which there exists no other nontrivial subgroup containing it > the factor group of a maximal subgroup is simple
commutator group [G,G]	= group generated form all group elements $xyx^{-1}y^{-1}$
Abelianization of G	= quotient G/[G,G]
def: [G,G]	$[G,G] := \langle [g_1,g_2] \| g_1,g_2 \in G\rangle$ *and where* $[g_1,g_2] := g_1g_2g_1^{-1}g_2^{-1}$.
2.4 extending groups	
2.4.1 (semi)direct products	
def: (outer) semidirect product	For groups N and H For homomorphism β: H→aut(N) > define the (outer) semidirect product of N and H with respect to β as: $N \rtimes_\beta H = \{(n,h) \| n,h \in N,H\}$: $(n_1,h_1)\cdot(n_2,h_2) := (n_1\cdot\beta_{h_1}(n_2), h_1\cdot h_2)$ where we have $(n,h)^{-1} = (\beta_{h^{-1}}(n^{-1}), h^{-1})$
def: inner semidirect product	For group G with normal subgroup N and subgroup H > G is the inner semidirect product of N and H if G is the outer semidirect product of N and H where the action of H on N is given by conjugation in G
2.4.2 sequences & extensions	
exact sequence	for group homomorphisms ϕ_i, define: $G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \longrightarrow \dots$ where we have the property that the image of the homomorphism ϕ_{k-1}: $G_{k-1}\to G_k$ must be the complete kernel of the homomorphism ϕ_k: $G_k\to G_{k+1}$ or thus: $\phi_k(\phi_{k-1}(x)) = 1, \forall x$ (with 1 = identity element!!)
short exact sequence	these are exact sequences of the form: $1 \longrightarrow N \xrightarrow{\phi_1} G \xrightarrow{\phi_2} G/N \longrightarrow 1$
extra property	if there exists a homomorphism ϕ between G and H in an exact sequence > then there also exists a homomorphism φ between H and G which return the element ie: φ(ϕ(g)) = g ∈ G for the inner semidirect product G=N⋊H

<table>
<tr>
<td>equivalent exact short sequences</td>
<td>two short sequences: $1 \longrightarrow N \xrightarrow{i} G_1 \xrightarrow{\pi} H \longrightarrow 1$
$1 \longrightarrow N \xrightarrow{i'} G_2 \xrightarrow{\pi'} H \longrightarrow 1$
are equivalent iff there exists a group isomorphism T: $G_1 \rightarrow G_2$ that makes the diagram:
commute

$$\begin{tikzcd} & & G_1 \arrow[dd, "T"] \arrow[dr, "\pi"] & & \\ 1 \arrow[r] & N \arrow[ur, "i"] \arrow[dr, "i'"'] & & H \arrow[r] & 1 \\ & & G_2 \arrow[ur, "\pi'"'] & & \end{tikzcd}$$

meaning that every path with the same start and end point defines the same map</td>
</tr>
<tr>
<td>cohomology group</td>
<td>For A an Abelian group and two groups G and H
look at the extension:

$$1 \longrightarrow A \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 1$$

we can define a multiplication rule:

$$(a_1, h_1) \cdot (a_2, h_2) := (a_1 + a_2 + \omega(h_1, h_2), h_1 h_2)$$

this again defines a group if we also require associativity:

$$\omega(h_1, h_2) + \omega(h_1 h_2, h_3) = \omega(h_1, h_2 h_3) + \omega(h_2, h_3)$$
</td>
</tr>
</table>