§ 1 Groups and actions

1. Permutation groups Let $X \neq \emptyset$ be a set and let $Sym(X)$ denote the collection of all bijective maps $\alpha : X \to X$. Then the $Sym(X)$ is a group (with respect to the composition of maps), the symmetric grp.
If X is finite, with cardinality $\# X = n$, then $Sym(X)$ has cardinality $\# Sym(X) = n!$ $= n \cdot (n-1)(n-2) \cdots 1$.
A subgroup $H \subseteq Sym(X)$ is called a permutation group (on the set X)

Ex For $p, q \in X$, $p \neq q$ let τ_{pq} denote the permutation that interchanges p and q, and fixes all other elements in X. Then τ_{pq} is called a transposition.

(a) let H denote the subgrp of $Sym(X)$ of all elements of $Sym(X)$ that can be written as a product of transpositions (why is this a subgrp? – Assume $\#X \geq 2$ ...)

If X is finite, then $H = \mathrm{Sym}(X)$ ($\rightarrow$ Algebra I)

If X is infinite, then $H \neq \mathrm{Sym}(X)$ (why?)

(b) Let $K \subseteq H$ denote the subgrp of all permutations that can be written as a product of an <u>even</u> number of transpositions.

Then $K \neq H$ (the <u>index</u> of K in H is $[H : K] = 2$). This is the <u>alternating grp</u>

$K = \mathrm{Alt}(X) \subseteq \mathrm{Sym}(X)$

2. <u>Actions</u> Let $X \neq \emptyset$ be a set and let G be a grp. An <u>action</u> of G on X is a map

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto gx \end{aligned}$$

such that the following hold:

(A1) $ep = p$ for all $p \in X$

e is neutral element in G

(A2) $g(hp) = (gh)p$ for all $g, h \in G$, $p \in X$

An equivalent (sometimes better) definition is as follows: an action is a homomorphism

$\varphi : G \to \mathrm{Sym}(X)$, put

$$gp = \varphi(g)(p)$$

The kernel of the action is $N = \{ g \in G \mid gp = p \text{ for all } p \in X \} = \ker(\varphi)$. This is a normal subgroup in G. The action is faithful if its kernel is trivial, $N = \{e\}$.

3 Example (a) $\mathrm{Sym}(X)$ acts on X via

$(\alpha, p) \longmapsto \alpha(p)$, with trivial kernel

(b) Put $X = G$, then G acts on X

via $(g, p) \longmapsto \underbrace{gp}_{\text{group multiplication}}$ $\quad g \in G$, $p \in G$

(the left regular action)

(c) Let $H \leq G$ be a subgroup, put $X = G/H$

$= \{ aH \mid a \in G \}$ left cosets

Then G acts on X via

$$(g, aH) \longmapsto gaH \qquad a, b \in G$$

(what is the kernel of this action? - the <u>largest</u> normal subgrp $N \trianglelefteq G$ with $N \leq H$)

(d) $X = G \qquad (g, p) \longmapsto gpg^{-1} = \gamma_g(p)$

this is the <u>conjugation action</u> of G on itself. This action has the additional property that $\gamma_g(pq) = \gamma_g(p)\gamma_g(q)$, i.e. we have a homomorphism $\varphi : G \to \mathrm{Aut}(G) \leq \mathrm{Sym}(G)$ into the <u>automorphism grp</u> of G

(what is the kernel of this action? - the center $\mathrm{Cen}(G)$ of G)

$\mathrm{Aut}(G) = \{ \alpha : G \to G \mid \alpha \text{ automorphism of } G \}$

$\mathrm{Cen}(G) = \{ z \in G \mid gz = zg \text{ for all } g \in G \}$

$\parallel$

$Z(G)$

4. Def Let $G \times X \to X$ be an action.

The stabilizer of $p \in X$ is the subgrp

$$G_p = \{ g \in G \mid gp = p \}$$

The orbit of $p \in X$ is the subset

$$G(p) = \{ gp \mid g \in \} \subseteq X$$

Lemma A The map $G/G_p \longrightarrow G(p)$

$$gG_p \longmapsto gp$$

is well-defined and bijective.

Pf If $a \in G_p$, then $(ga)p = g(ap) = g(p)$, hence the map is well-defined.

Clearly, it is surjective.

Suppose that $gp = hp$. Then $(h^{-1}g)p = p$, whence $h^{-1}g \in G_p$, hence $gG_p = hG_p$.

Thus, it is injective $\square$

<u>Lemma B</u> For $q = gp$ we have

$$G_q = g G_p g^{-1}.$$

<u>Pf</u> We have $h(gp) = gp \Leftrightarrow g^{-1}hgp = p$

$$\Leftrightarrow g^{-1}hg \in G_p \Leftrightarrow h \in g G_p g^{-1} \qquad \square$$

<u>Corollary</u> If $G \times X \to X$ is an action, and if $N \trianglelefteq G$ fixes some $p \in X$, then N fixes every $q \in G(p)$.

<u>Lemma C</u> The orbits of an action partition the set X, that is: for $p, q \in X$ we have either $G(p) = G(q)$ <u>or</u> $G(p) \cap G(q) = \phi$.

<u>Pf</u> Suppose $z \in G(p) \cap G(q)$. Then there are $a, b \in G$ with $z = ap = bq$. For $g \in G$ we have then $gq = g(b^{-1}a)p \in G(p)$, whence $G(q) \subseteq G(p)$. Similarly, $G(p) \subseteq G(q)$.

$\square$

5. Definition The orbit space of an action $G \times X \to X$ is the set of orbits,

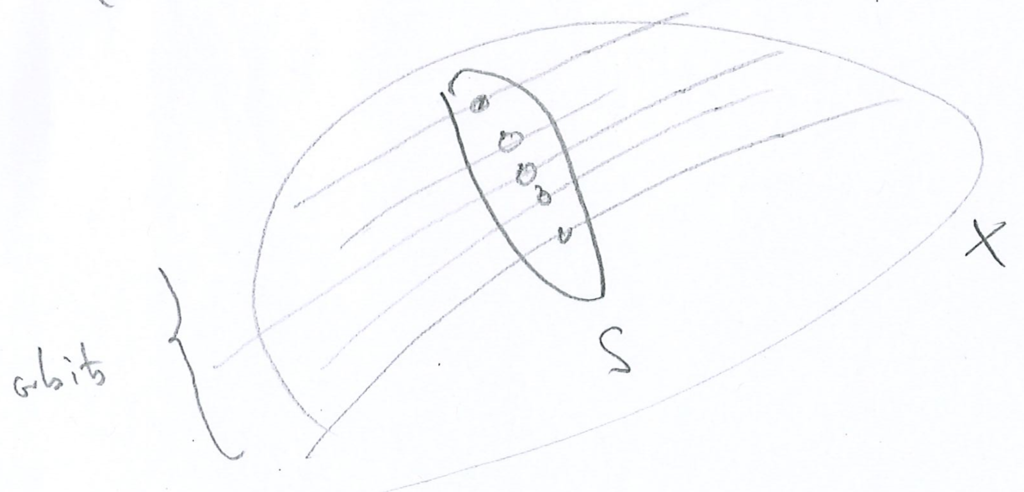
$$G\backslash X = \{ G(p) \mid p \in X \}$$

There is a natural map $X \to G\backslash X$, $p \mapsto G(p)$.

A cross section is a subset $S \subseteq X$ such that S intersects every orbit in exactly one element. It follows that

$$\# X = \sum_{s \in S} \# G(s) = \sum_{s \in S} [G : G_s]$$

(Cross sections exist always by the axiom of choice)



6. <u>Def</u> An action $G \times X \to X$ is <u>transitive</u> if it satisfies one of the following equivalent conditions.

(i) For all $p, q \in X$ there is $g \in G$ with $gp = q$

(ii) For all $p \in X$ we have $G(p) = X$

(iii) For some $z \in X$ we have $G(z) = X$

<u>pf</u> (of the equivalence)

(i) $\Rightarrow$ (ii) clear, (ii) $\Rightarrow$ (iii) clear

(iii) $\Rightarrow$ (i) : Put $p = az$, $q = bz \Rightarrow q = ba^{-1}p$ $\square$

<u>Examples</u> (a) $Sym(X) \times X \to X$ is transitive

(b) $G \times G/H \to G/H$, $(g, aH) \mapsto gaH$ is transitive

(c) If $G \neq \{e\}$, then the conjugation action

$G \times G \to G$, $(g, p) \longmapsto gpg^{-1}$

is <u>not</u> transitive, because the orbit of e is $\{e\} \neq G$ $\quad$ ($geg^{-1} = e$ for all $g \in G$)

7. Def An action $G \times X \to X$ is called sharply transitive or regular or simply transitive if it is transitive, and if for some (every) $p \in X$ we have $G_p = \{e\}$.
Thus, the map $G \to X$, $g \mapsto gp$ is a bijection.

Ex The left regular action

$$G \times G \to G \quad , (g, a) \longmapsto ga$$

is sharply transitive.

8. Remark: left vs right

A right action of a gp is a map

$$\begin{aligned} X \times G &\to X \\ (p, g) &\mapsto p^g \end{aligned}$$

such that the following hold:

(RA1) $p^e = p$ for all $p \in X$

(RA2) $p^{(gh)} = (p^g)^h$ for all $p \in X$, $g, h \in G$.

There is a bijective correspondence between left and right action as follows:

(i) $G \times X \to X$ (left) action

put $p^g := g^{-1}p \rightsquigarrow$ right action

(ii) $X \times G \to X$ right action

put $gp = p^{(g^{-1})} \rightsquigarrow$ left action

Ex G grp, $H \leq G$ sub grp, H acts on G from the right via $p^h = ph$ $\quad p \in G$, $h \in H$

The orbit of $a \in G$ is the left coset aH.

The orbit space of this action is $G/_H = \{aH \mid a \in G\}$

9. Def Let $H \leq G$ be a sub grp in the grp G. The index of H in G is the cardinality

$[G:H] = \#(G/_H)$ (which may be finite or infinite).

Lagrange's Theorem says: $\#G = [G:H] \cdot \#H$

Proof: For every $a \in G$ we have $\# aH = \# H$, because $h \mapsto ah$ is a bijection $H \to aH$.

Since G is the disjoint union of the cosets $aH \subseteq G$ we have $\# G = [G:H] \cdot \# H$

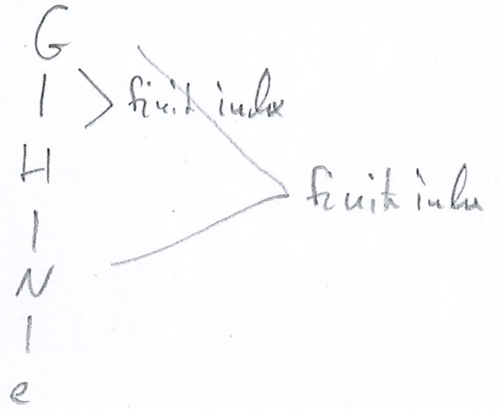
[This is the formula on page 7]

Cor If two of the three cardinalities $\#G$, $\#H$, $[G:H]$ are finite, then all of them are finite.

Ex $G = (\mathbb{Z}, +)$, $H = 3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \dots\}$

$[G:H] = 3$, but G and H are infinite.

10. <u>Proposition</u> (<u>Poincaré's Lemma</u>). Let H be a subgrp of G. If $[G:H]$ is finite, then there is a normal subgrp $N \trianglelefteq G$ with $N \subseteq H$ and $[G:N]$ is still finite.



<u>PF</u> The grp G acts on the <u>finite</u> set $X = G/H$ via $(g, aH) \longmapsto gaH$.

Hence we have a homomorphism

$$f : G \to \underset{\text{finite}}{\mathrm{Sym}(X)}$$

Put $N = \ker(f)$. Then $f(G) \cong G/N$ is finite, hence $[G:N] \leq \# \mathrm{Sym}(X)$ $\square$

We have used the <u>Homomorphism Theorem</u>:

If $f : G \to K$ is a grp homomph, with kernel N, then f factors as

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & K \\ & G/N \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

$\pi(g) = gN$, $\bar{f}(gN) = f(g)$

and $\bar{f}$ is injective, $f(G) \cong \bar{f}(G/N) \cong G/N$ $\square$

11. Generation of (sub)groups

Let G be a group, let $S \subseteq G$ be a subset. We call

$$\langle S \rangle = \bigcap \{ H \subseteq G \mid H \text{ subgrp and } S \subseteq H \}$$

the subgrp generated by S. (So $\langle \emptyset \rangle = \{e\}$).

<u>Lemma</u> Put $S^* = S \cup \{e\} \cup S^{-1}$, where $S^{-1} = \{ s^{-1} \mid s \in S \}$. Then

$$\langle S \rangle = \{ g_1 \cdots g_n \mid n \geq 1,\ g_1, \dots, g_n \in S^* \}$$

Pf $g_1, \dots, g_n \in S^* \Rightarrow g_1, \dots, g_n \in \langle S \rangle$

$$\Rightarrow \underbrace{\{ g_1 \cdots g_n \mid n \geq 1, g_1, \dots, g_n \in S^* \}}_{= H} \subseteq \langle S \rangle.$$

Conversely, H is a subgrp ($g \in S^* \Rightarrow g^{-1} \in S^*$, $e \in S^*$, $g, h \in S^* \Rightarrow gh \in H$) and $S \subseteq H$, hence $\langle S \rangle \subseteq H$. $\square$

#

If $\langle S \rangle = G$, then S is called a generating set for G. A grp G is called finitely generated if there is a finite set $S \subseteq G$ with $\langle S \rangle = G$.

Ex (a) every finite group is finitely generated (put $S = G$)

(b) $(\mathbb{Z}, +)$ is finitely generated, put $S = \{1\} \Rightarrow S^* = \{1, 0, -1\}$

(c) $(\mathbb{Q}, +)$ is not finitely generated (homework)

Note: every finitely generated grp is countable.

12. <u>Lemma</u> Let $f: G \to K$ be a homomorphism. If $S \subseteq G$ generates G, then $f(S) \subseteq K$ generates $f(G) \subseteq K$.

<u>Pf</u> We have $f(S^*) = f(S)^*$, every $g \in G$ is of the form $g = g_1 \cdots g_n$, $g_1, \dots, g_n \in S^*$

$\Rightarrow f(g) = f(g_1) \cdots f(g_n)$ $f(g_1), \dots, f(g_n) \in f(S)^*$ $\square$

<u>Cor</u> If $f: G \to K$ is a homomorphism and if G is finitely generated, then $f(G) \subseteq K$ is finitely generated.

13. <u>Theorem</u> Let $H \subseteq G$ be a subgroup in G of finite Index $m = [G:H]$. The following are equivalent:

(i) H is finitely generated.

(ii) G is finitely generated.

<u>Pf</u> Put $G = g_1 H \cup g_2 H \cup \dots \cup g_m H$, $g_1 = e$

(i) $\Rightarrow$ (ii): If $S = \{s_1, \dots, s_n\}$ generates H, then $\{s_1, \dots, s_n, g_1, \dots, g_m\}$ generates G.

(ii)$\Rightarrow$(i): for each $g \in G$ there is a unique i s.t. $gH = g_i H$. Put $\bar{g} = g_i$ and note that $\bar{\bar{g}} = \bar{g}$. Since $gH = \bar{g}H$, we have $\bar{g}^{-1} g \in H$. For $h \in H$ we have $\bar{h} = e = g_1$.

Also, $abH = a\bar{b}H = \overline{a\bar{b}}H$ hence $\overline{ab} = \overline{a\bar{b}}$.

Let S be a finite generating set for G and put

$$T = \{ \overline{ag_i}^{-1} \cdot ag_i \mid a \in S^*,\ 1 \le i \le m \}.$$

Let $h \in H$, $h = a_1 \cdots a_k$, $a_j \in S^*$.

$$\begin{aligned}
h &= a_1 \cdots a_k \\
&= a_1 \cdots a_{k-1}\, \bar{a}_k \underbrace{\bar{a}_k^{-1} a_k}_{= b_k} && b_k \in T \\
&= a_1 \cdots a_{k-2} \cdot \overline{a_{k-1}\bar{a}_k} \cdot \underbrace{\overline{a_{k-1}\bar{a}_k}^{-1} \cdot a_{k-1}\bar{a}_k}_{= b_{k-1}} \cdot b_k && b_{k-1} \in T \\
&\ \ \vdots \\
&= a_1 \overline{a_2 \cdots \overline{a_{k-1}\bar{a}_k}}\, b_2 \cdots b_k && b_2 \cdots b_k \in T \\
&\overset{(!)}{=} \underbrace{\overline{a_1 \overline{\cdots \bar{a}_k}} \cdot \overline{a_1 \overline{\cdots \bar{a}_k}}^{-1} \cdot a_1 \overline{a_2 \cdots \bar{a}_k}}_{= b_1}\, b_2 \cdots b_k && b_1 \in T
\end{aligned}$$

because

$$\overline{\overline{a_1}\,\overline{a_2}\cdots\overline{a_k}} = \overline{a_1\cdots a_k} = e, \text{ since } a_1\cdots a_k \in H$$

$\square$

It is in general not true that a subgrp of a f.g. group is again finitely generated! (→ later...)

13. Def A group G is noetherian (→ E. Noether) if every countably infinite chain of subgrps

$$H_0 \subseteq H_1 \subseteq H_2 \subseteq \dots \leq G$$

becomes constant after finitely many steps, i.e. $H_{m+k} = H_m$ for all $k \geq 0$, for some $m \geq 0$. Every finite group is noetherian, obviously.

Lemma A group G is noetherian if and only if every subgrp $H \leq G$ is finitely generated.

Pf Suppose that G is noetherian and that $H \leq G$ is not finitely generated. For all $h_0, \dots, h_k \in H$, there is hence an element $h_{k+1} \in H - \langle h_0, \dots, h_k \rangle$.

Put $H_k = \langle h_0, \dots, h_k \rangle$, then

$$H_0 \subsetneq H_1 \subsetneq H_2 \subsetneq \dots$$

is an infinite ascending chain

of subgrps, hence G is not noetherian.

Suppose that G is not noetherian. Then there is an infinite chain of subgrps $H_0 \subsetneq H_1 \subsetneq H_2 \subsetneq \dots$.

Put $H_\infty = \bigcup_{k=0}^{\infty} H_k$, then H_∞ is a subgrp (why?). Given $h_0, \dots, h_m \in H_\infty$, there is ℓ with $h_0, \dots, h_m \in H_\ell \Rightarrow \langle h_0, \dots, h_m \rangle \subseteq H_\ell \subsetneq H_\infty$, hence H_∞ is not finitely generated. $\square$

14. <u>Proposition</u> (i) Subgrps and quotients of noetherian grps are again noetherian.

(ii) If $N \trianglelefteq G$ is normal and if G/N and N are noetherian, then G is noetherian.

<u>pf</u> Suppose that G is noetherian, and that $H \leq G$ is a subgrp. Then every subgrp of H is finitely generated, hence H is noetherian.

If $N \trianglelefteq G$ and if G/N is <u>not</u> noetherian, then G is <u>not</u> noetherian [$K_0 \subsetneq K_1 \subsetneq \dots \subseteq G/N$

Consider $\pi: G \to G/N$, $H_k = \pi^{-1}(K_k) \Rightarrow$

$H_0 \subsetneq H_1 \subsetneq H_2 \dots$]

(ii) Let $H_0 \subsetneq H_1 \subsetneq \dots$ in G be an infinite ascending chain. If $N \trianglelefteq$ is noetherian, then there is m such that $H_{k+m} \cap N = H_m \cap N$ for all $k \geq 0$.
If G/N is noetherian, then there is l such that

$$H_{k+l} N = H_k N \quad \text{for all } k \geq 0.$$

$\Rightarrow$ We may assume $\underline{m = l}$.

Claim: $H_m = H_{m+k}$ for all $k \geq 0$

Otherwise, $h \in H_{m+k} - H_m$. Then

$hN = \tilde{h}N$ for some $\tilde{h} \in H_m \Rightarrow \tilde{h} = hn$ for some $n \in N$. Hence $n \in H_{m+k} \cap N = H_m \cap N$

$\Rightarrow h \in H_m$ ↯ $\square$

15. Corollary Every finitely generated abelian group G is noetherian.

pf: Let n be the minimum number of generators for G. $\boxed{n=0} \Rightarrow G = \{e\}$ ✓

$\boxed{n=1} \Rightarrow G = \langle g \rangle$ is a cyclic group.

Let $H \leq G$ be a subgrp. Then $g^l \in H$ for some

$l \geq 1$ minimal. If $h \in H$, then $h = g^m$

$= g^{sl+t}$, $0 \leq t < l \Rightarrow g^t \in H \Rightarrow t = 0$

hence $H = \langle g^l \rangle$, so H is finitely generated.

$\boxed{n \geq 2}$ $G = \langle g_1, \ldots, g_n \rangle$, put $K = \langle g_2, \ldots, g_n \rangle$,

$L = \langle g_1 \rangle$, consider $\pi : G \to G/L$. Then

$\pi(g_2), \ldots, \pi(g_n)$ generate G/L. By induction,

G/L is noetherian and L is noetherian $\Rightarrow$ G is

noetherian. $\square$

16. Def A group G is called hopfian ($\to$ H. Hopf)

if every surjective homomorphism $\varphi : G \to G$

is bijective.

Ex: Every finite group is Hopfian. ‡

Proposition Every noetherian group is

hopfian.

proof Put $N_j = \ker(\varphi^j)$ for $j = 0, 1, 2, 3 \ldots$
($\varphi^0 = id_G$, $N_0 = \{e\}$). Then

$N_0 \subseteq N_1 \subseteq \ldots$ is an ascending chain of subgrps.

Assume $N_1 = \ker(\varphi) \neq \{e\}$.

Claim: $\varphi(N_{j+1}) = N_j$

$g \in N_{j+1} \Rightarrow \varphi^j \varphi(g) = e$ (✓) $\Rightarrow \varphi(N_{j+1}) \subseteq N_j$

$h \in N_j \Rightarrow h = \varphi(g)$ for some g because φ is surjective

$\varphi^j(h) = e = \varphi^{j+1}(g) \Rightarrow g \in N_{j+1} \Rightarrow \varphi(N_{j+1}) \supseteq N_j$ $\square$

Hence $N_{j+1}/N \cong N_j$ by the homomorphism theorem.

Now $$N_{j+1}/N_j \cong \frac{N_{j+2}/N}{N_{j+1}/N} \cong N_{j+2}/N_{j+1}$$

hence $N_{j+1}/N_j \cong N$ for all $j \geq 0$

If $N \neq \{e\}$, then $N_{j+1} \supsetneq N_j$ for all j

$\Rightarrow$ G is not noetherian if it is not hopfian.

$\square$

Recall the Isomorphism Theorems:

(1) $H, N \leq G$ subgroups with $N \trianglelefteq G$.

Then $\pi : G \to G/N$ induces an isomorphism

$$H/_{H \cap N} \xrightarrow{\cong} HN/_N$$

$$h(H \cap N) \longmapsto hN$$

(2) $K, N \trianglelefteq G$ normal subgroups, $N \leq K \leq G$.

Then $f : G/N \to G/K$ induces an isomorphism

$$\frac{G/N}{K/N} \xrightarrow{\cong} G/K$$

Homomorphism Theorem: $f : G \to K$ a homomorphism, with kernel $N = \ker(f)$. Then there is a unique homomorphism $\bar{f} : G/N \to K$ such that $f = \bar{f} \circ \pi$,

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & K \\ G/N \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

and $\bar{f}$ induces an isomorphism

$$G/N \xrightarrow{\bar{f}} f(G)$$