6.E Operation of Groups

In many situation "symmetries" play an important roll. In general this lead to prove invariant-properties with respect to the operation of a group. In this subsection explore the elementary concepts pertinent to this subject.

Let G be a group and let X be a set. We recall that an (left)-operation of the set G on X is a map $G \times X \longrightarrow X$. We write it in general in the form

$$(g, x) \longmapsto gx, \quad g \in G, \; x \in X.$$

For a fixed $g \in G$, the map $X \longrightarrow X$, $x \longmapsto gx$, from X into itself is called the operation of g on X and is denoted by ϑ_g. The following definition further demand that the operation of G on X is compatible with the group structure of G

(See page 6E/1-a)

6.E.1 Definition* An (left)-operation of a (group) G on the set X, $G \times X \longrightarrow X$, $(g, x) \longmapsto gx$ is called an operation (or an action) of G as group, if for all $g, h \in G$ and all $x \in X$

We have: (1) $e_G \cdot x = x$ (2) $(gh)x = g(hx)$.
The *operation* of $g \in G$ on X is the map $\vartheta_g : X \longrightarrow X$, $x \longmapsto gx$. Then, the above conditions (1) and (2) are equivalent to (1') $\vartheta_{e_G} = \mathrm{id}_X$ and (2') $\vartheta_{gh} = \vartheta_g \circ \vartheta_h$. In particular, ϑ_g is a permutation on X with inverse $(\vartheta_g)^{-1} = \vartheta_{g^{-1}}$. Therefore the map $\vartheta : G \longrightarrow \mathfrak{S}(X)$, $g \longmapsto \vartheta_g$, is a group homomorphism. Conversely, if $\vartheta : G \longrightarrow \mathfrak{S}(X)$ is a group homomorphism, then the map $G \times X \longrightarrow X$, $(g,x) \longmapsto gx := \vartheta(g)(x)$ is an operation of G on X.

A set X with an operation of a group G (from left) is called a *G-set* or a *G-space* and the group homomorphism $\vartheta : G \longrightarrow \mathfrak{S}(X)$ belonging to it is called the *action homomorphism* of the G-set X. The kernel of ϑ, i.e. the set of $g \in G$ with $\vartheta_g = \mathrm{id}_X$ or with $gx = x$ for all $x \in X$, is called the *kernel of the operation*. If this kernel is trivial, then the action is called *faithful* or *effective*. If this kernel is the whole group G, i.e. if $gx = x$ for all $g \in G$ and all $x \in X$, then the operation is called the *trivial operation*.
Any faithful operation can be identified with the canonical operation of a subgroup of a

Therefore, a right operation of G is the same as a left operation of G^{op} (and conversely).

* The study of sets with group operation was initiated by Felix Klein in his famous Erlanger Program "Vergleichende Betrachtungen über neuere geometrische Forschungen" from 1872, whereby Klein considered only transformation groups (see also Footnote on page 6E/3), especially Lie groups occurring as transformation groups. His main examples were derived from projective groups and their subgroups operating canonically on projective spaces. The more general concept we introduce here goes back basically to Hermann Weyl. So special cases occurred already in 1854 in the work of Arthur Cayley on abstract Group Theory.

† An operation from the right of a group G on the set X is a map $X \times G \longrightarrow X$, $(x, g) \longmapsto xg$ with $xe = x$ and $x(gh) = (xg)h$ for all $g, h \in G$ and all $x \in X$. If $(x,g) \longmapsto xg$ is an operation from right, then $(g,x) \longmapsto gx := xg^{-1}$ is an operation from the left, and conversely. Therefore in principle left and right operations are interchangable. For a right operation $X \times G \longrightarrow X$ the action homomorphism $\eta : G \to \mathfrak{S}(X)$, $g \longmapsto \eta_g : x \longmapsto xg$, is an anti-homomorphism of groups: $\eta(gh) = \eta_{gh} = \eta_h \circ \eta_g = \eta(h) \cdot \eta(g)$ for all $g, h \in G$, i.e. a homomorphism $G^{op} \longrightarrow \mathfrak{S}(X)$, from the

permutation group obtained by restricting the canonical operation $\mathfrak{S}(X)\times X \longrightarrow X$, $(\sigma, x) \longmapsto \sigma(x)$ of $\mathfrak{S}(X)$ on X. An arbitra operation of G with action homomorphism ϑ induces canonically a faithful operati of $G/\mathrm{Ker}\,\vartheta$. Note that the kernel $\mathrm{Ker}\,\vartheta$ of the operation is the intersection of all stabilizers G_x, $x\in X$, i.e. $\mathrm{Ker}\,\vartheta = \bigcap_{x\in X} G_x$.

The operation of a group G on the set X defines in a natural way an equivalence relation $\sim_G$ on X: Elements $x, y\in X$ are related under $\sim_G$ if y is obtained from x by the operation ϑ_g for some $g\in G$, i.e. $x\sim_G y$ if and only if $y = gx$ for some $g\in G$. This is indeed an equivalence relation as easily checked by using the conditions (1) and (2) of a group operation: $e_G\cdot x = x$, i.e. $x\sim_G x$; from

[1] Historically, by definition groups were transformation groups, i.e. subgroups of permutation groups of sets with their canonical operations. In particular, symmetry groups were considered as such transformation groups operating on the structures under consideration. Such symmetry groups particularly the continuous Lie groups, play an important role in many academic disciplines for example can be used to understand fundamental physical laws underlying special relativity and symmetry

$y = gx$, if $x = g^{-1}y$ follows, i.e. $x \sim_G y \Rightarrow y \sim_G x$; finally, from $y = gx$ and $z = hy$, the equality $z = h(gx) = (hg)x$, i.e. $x \underset{G}{\sim} z$ follows.

The equivalence class $Gx := \{gx \mid g \in G\}$ of an element $x \in X$ under $\sim_G$ is called the G-orbit of x. The orbit-space of X (with respect to the given operation of G), i.e. the set of all orbits Gx, $x \in X$, is denoted by $X \backslash G$.

For $x \in X$, to understand the orbit Gx of x, we consider the canonical surjective map $G \longrightarrow Gx$, $g \longmapsto gx$ from G onto the orbit Gx of x. Two elements $gx = hx$ if and only if $h^{-1}(gx) = x$, or, equivalently, h and g belong to the same left-coset of the well-known isotropy group or stabilizer of $x \in X$:

$$G_x := \{g \in G \mid gx = x\}.$$

G_x is clearly a subgroup of G; consisting those elements g of G for which x is a fixed point of ϑ_g, i.e. $G_x = \{g \in G \mid x \in \mathrm{Fix}_{\vartheta_g} X\}$.

The ~~point~~ $x \in X$ is called a fixed point of the operation of G if $x \in \bigcap_{g \in G} \mathrm{Fix}_{\vartheta_g} X$, or equivalently, $G_x = G$. The set of all fixed points of the operation of G on X, is denoted by $\mathrm{Fix}_G X$ or X^G.

In any case the fibres of the canonical surjective map $f_x : G \longrightarrow Gx$, $g \longmapsto gx$, are the left-cosets of G_x in G, i.e

$$f_x^{-1}(gx) = \{h \in G \mid hx = gx\} = \{h \in G \mid g^{-1}hx = x\}$$
$$= gG_x .$$

This proves the following important theorem which is used very often:

6.E.2 Theorem (Orbit-Stabilizer Theorem)

Let G be a group which operates on the set X. Then the cardinality $\#Gx$ of the orbit Gx of $x \in X$ is the index $[G:G_x] := \#(G/G_x)$ of the stabilizer G_x of x in G, i.e.

$$\#Gx = [G:G_x].$$

In particular, if G is finite, then the cardinality $\#Gx$ of Gx divides the order $\#G$ of G. Furthermore, the stabilizers of the elements in the same orbit are conjugate subgroups, more precisely,

$$G_{gx} = g G_x g^{-1}, \; g \in G, \; x \in X.$$

Proof The surjective map $f_x : G \to Gx$, $g \mapsto gx$, induces a bijective map

$$G/G_x \xrightarrow{\approx} Gx, \; gG_x \longmapsto gx.$$

Further, for $g \in G$ and $x \in X$, $h \in G_{gx}$, i.e. $h(gx) = gx$ if and only if $g^{-1}hgx = x$, i.e. $g^{-1}hg \in G_x$, or equivalently, $h \in gG_xg^{-1}$.

We remark that $\# Gx$ divides $\# G$ in case G is finite follows from the general equality $[G:H] \cdot \# H = \# G$ for any subgroup H of a finite group which again consequence of the following: All cosets gH (of H in G) have the same cardinality, since the map $H \to gH$, $h \mapsto gh$ are bijective. Further, (Lagrange's Theorem) The order of a subgroup of a finite group divides the order of the group.

If X is finite and if we count the elements of X with the help of orbits of X of a G-operation on X, then we get:

6.E.3 Class-Equation Let G be a group and let X be a finite set. If G operates on X, then:

$$\#X = \sum_{Gx \in X\backslash G} \#Gx = \sum_{Gx \in X\backslash G} [G : G_x]$$

$$= \#\mathrm{Fix}_G X + \sum_{\substack{Gx \in X\backslash G \\ Gx \neq \{x\}}} [G : G_x].$$

A group operation $G \times X \longrightarrow G$ is called transitive if it has exactly one orbit, i.e if $X \neq \phi$ and if $Gx = X$ for one $x \in X$ and hence for all $x \in X$. Equivalently, if $X \neq \phi$ and if for arbitrary $x, y \in X$, there exists $g \in G$ with $y = gx$. A set X with a transitive operation of the group G is also called a homogeneous G-space.

A group operation $G \times X \longrightarrow X$ is called free if the isotropy group G_x is trivial for every $x \in X$. It is called simply-transitive if it is transitive and free, i.e. if $X \neq \phi$ and if for arbitrary $x, y \in X$ there exists unique $g \in G$ with $y = gx$. Equivalently, if it is transitive and if one and hence all isotropy groups G_x, $x \in X$, are trivial. If the operation $G \times X \longrightarrow X$ is simply-transitive, then for every $x \in X$, the map $G \longrightarrow X$, $g \longmapsto gx$, is bijective.

<u>6.E.4 Example</u> (<u>Left regular</u> or <u>the Cayley operation</u>) The binary operation $G \times G \longrightarrow G$ in an arbitrary group G is the most natural operation of G onto itself; it is simply transitive. The corresponding action homomorphism $\vartheta : G \to \mathfrak{S}(G)$ maps g to the left multiplication $\lambda_g : G \to G$, $x \longmapsto gx$, $x \in G$. This operation is called the (<u>left</u>) <u>regular operation</u> or the <u>Cayley operation</u> of G onto itself. The injective homomorphism $\lambda : G \longrightarrow \mathfrak{S}(G)$, $g \mapsto \lambda_g$, is called the <u>Cayley-representation</u> of G as transformation group, see 5.A.11.

If we restrict this operation of G to the subgroup H of G, i.e. if we consider the operation $H \times G \longrightarrow G$, $(h, g) \longmapsto hg$ of H on the set G, then the H-orbits are the <u>right-cosets</u> (of H in G) $Hg = \{hg \mid h \in H\}$, $g \in G$ and the isotropy groups $H_x = \{h \in H \mid hx = x\}$ are trivial, $x \in G$.

Therefore it follows from the class-equation 6.E.3 that:

(<u>Lagrange's Theorem</u>) $\# G = \#(G\backslash H)\,\# H$.

The <u>left-cosets</u> (of H in G) $gH := \{gh \mid h \in H\}$ are the H-orbits of the restriction of the right operation $G \times G \longrightarrow G$, $(x,g) \mapsto xg$ to the right operation $G \times H \longrightarrow G$, $(g,h) \mapsto gh$ of H on G. In this case the orbit-space is denoted by G/H. More generally, the (right) orbit space is denoted by X/G.

6.E5 Example (Conjugation-Operation)

A somewhat less canonical example of an operation of a group G onto itself is the <u>Conjugation operation</u>: $G \times G \longrightarrow G$, $(g,x) \longmapsto gxg^{-1}$, $g \in G$, $x \in X$. The corresponding action homomorphism

$\kappa : G \longrightarrow \mathrm{Aut}\, G \subseteq \mathfrak{S}(G)$, $g \longmapsto \kappa_g \in \mathrm{Aut}\, G$,

---

1 While Lagrange did not have the group concept -- not even that of a group of permutations -- he was the first to realize the significance of the study of permutations of the roots in the theory of equations. Moreover, his work on the theory of equations in 1770 stimulate the later work Cauchy and Galois and contained in essence the proof of what we call now Lagrange's theorem

Where $\kappa_g : G \longrightarrow G$ is the inner-automorphism $x \longmapsto gxg^{-1}$ of G by g. The orbits of this operation on G are called the conjugacy classes in G and the fixed pointset $\mathrm{Fix}_G G$ is the center $Z(G) := \{x \in G \mid gx = xg \text{ for all } g \in G\}$ which is also the kernel of the action, i.e. $\mathrm{Ker}\,\kappa = Z(G)$. Moreover, if G is finite, then the class-equation of G is:

$$\# G = \# Z(G) + \sum_{i=1}^{r} \# C_i \text{, where}$$

$C_1, \ldots, C_r$ denote the distinct conjugacy classes with cardinality > 1. If $x_i \in C_i$, $i = 1, \ldots, r$, then $\# C_i = [G : C_G(x_i)]$, where, for $x \in G$, $C_G(x) := \{g \in G \mid gx = xg\}$ is the subgroup of those elements $g \in G$ which commute with x; it is called the centraliser of x in G. Note that the numbers $\# Z(G)$ and $\# C_i$, $i = 1, \ldots, r$, are all divisors of the order $\# G$ of the group G. The number of (all) conjugacy classes, i.e. $\# Z(G) + r$ is called the class-number of G.

As an application we note the following:

6.E.6 Theorem Let G be a non-trivial finite p-group, p prime, i.e. $\# G = p^m$ with p-prime and $m \in \mathbb{N}^*$. Then G has a non-trivial center.

Proof Since $\# G = p^m$, in the above class-equation in Example 6.E.4, $\# G$ as well as all other terms $\# C_i$, $i = 1, \ldots, r$, are divisible by p and hence p divides $\# Z(G)$, in particular, $Z(G) \neq \{1\}$.

More generally, from the class-equation in 6.E.3 it follows that:

6.E.7 Theorem Let G be a finite p-group, i.e. $\# G = p^m$ with p prime number and $m \in \mathbb{N}^*$ which operates on a finite set X. Then the congruence

$$\# X \equiv \# \mathrm{Fix}_G X \pmod{p}.$$

holds.

6.E.8 Example Let G be a finite group of order n and p be a prime number. On the set G^p of p-tuples of G, the cyclic group $\mathbb{Z}_p$ operates by:

$(a,(x_1,\dots,x_p)) \longmapsto (x_{1+a},\dots,x_{p+a})$, where the sum with a and the indices $1,\dots,p$ is the addition in the group $\mathbb{Z}_p$. The fixed points of this operation are the constant tuples $(x,\dots,x)$. Since, if $(x_1\cdots x_p)=(x_1\cdots x_r)(x_{r+1}\cdots x_p)=e$, then we also have $(x_{r+1}\cdots x_p)(x_1,\dots,x_r)=e$ for all $r=1,\dots,p-1$. Therefore the subset $X=\{(x_1,\dots,x_p)\in G^p \mid x_1\cdots x_p=e\}$ of G^p is $\mathbb{Z}_p$-invariant. From the class-equation of the $\mathbb{Z}_p$-set X, we get:

$$n^{p-1}=\#X \equiv \#\operatorname{Fix}_{\mathbb{Z}_p} X \pmod p.$$

Therefore if p divides n, then p also divides $\#\operatorname{Fix}_{\mathbb{Z}_p} X$. In particular, there exists $x\in G$, $x\neq e$ such that $x^p=e$.

This proves the following well-known theorem of Cauchy:

<u>**6.E.9 Theorem**</u> (<u>Cauchy</u>) A finite group G contains an element of order p for every prime divisor p of $\#G$.

Furthermore, if p does not divide n, then $\operatorname{Fix}_{\mathbb{Z}_p} X=\{(e,e,\dots,e)\}$ by Lagrange's theorem and hence the well-known consequence: (<u>Fermat's Little Theorem</u>): $n^{p-1}\equiv 1 \pmod p$.

Exercises

1. The kernel of an operation of a group G on a set X is the intersection of all isotropy groups G_x, $x \in X$. -- If G is abelian, then G operates simply-transitively if and only if G operates transitively and faithfully.

2. Let p be a prime number. Show that every group of order p^2 is abelian. Moreover, either it is cyclic or isomorphic to product of two cyclic groups of order p. (Hint: Use 6.E.6.)

3. Let p be a prime number. Show that every group of order $2p$ is either cyclic or isomorphic to the dihedral group D_p. ($p=2$ is a special case. For a generalisation see the Remarks in 7.A, Exercise 23)

4 Let p be a prime number and let G be a group of order p^3. Show that:
a) The commutator group of G and the

Center of G are equal, i.e.

$$[G:G] = Z(G).$$

(<u>Hint</u>: Apply Exercise 4 of 6.A.)

b) The class number of G is p^2+p-1.

(<u>Remark</u> Upto isomorphism there are two non-abelian groups and three abelian groups of order p^3, the abelian are: $\mathbb{Z}_{p^3}$, $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ and $(\mathbb{Z}_p)^3$, see Theorem 8.C.12.)

<u>5</u> For a group N, the map

$$(n,\sigma) \longmapsto \lambda_n \sigma, \; n \in N, \; \sigma \in \operatorname{Aut} N$$

is an injective homomorphism from $\operatorname{Hol}(N) = N \rtimes \operatorname{Aut} N$ into the permutation group $\mathfrak{S}(N)$, see Example 6.E.10, here λ_n denote the left translation $N \longrightarrow N$, $x \longmapsto nx$, by $n \in N$.)

<u>6</u> Let H be a subgroup of the group G. Then G operates transitively on the set G/H of left-cosets of H in G. The kernel of this operation $N := \bigcap_{g \in G} gHg^{-1}$. This is the biggest normal

subgroup of G contained in H.

In particular, this operation of G induce an injective group homomorphism from G/N into the permutation group $\mathfrak{S}(G/H)$.

Deduce that:

(1) Every subgroup of finite index n in G contains a normal subgroup of finite index which divide $n!$.

(2) If G is simple and $H \neq G$, then G is isomorphic to a subgroup of $\mathfrak{S}(G/H)$. In particular, Ord G divides $n!$, when H is of finite index $n > 1$ in G.

(3) If G is finite and H is a subgroup of prime index p, where p is the smallest prime divisor of Ord G, then H is normal in G. In particular, every subgroup of index p is normal in every group of an order p^m, $m \in \mathbb{N}^*$.

7. Let G be a group. Then G operates on the power set $\mathfrak{P}(G)$ of G by conjugation. For a subset A of G, the isotropy group G_A with respect to this operation is the normaliser of A in G and is denoted by $N_G(A)$. Show that $N_G(A)$

is the biggest subgroup of G which operates on A by conjugation. The kernel of this operation of $N_G(A)$ on A is the well-known <u>centraliser</u>

$$C_G(A) = \bigcap_{a \in A} C_G(a)$$

of A. In particular, $C_G(A)$ is normal in $N_G(A)$. If H is a subgroup of G, then $N_G(H)$ is the biggest subgroup of G such that H is normal in $N_G(H)$. The index $[G : N_G(H)]$ is the number of conjugate subgroups of H in G and divides $[G:H]$ if $[G:H]$ is finite.

<u>8</u>. Let G be a group and $H \neq G$ be a subgroup of finite index. Then

$$\bigcup_{x \in G} x H x^{-1} \neq G.$$ (<u>Hint</u>: Use Exercise 7)

<u>9</u>. Let G and H be finite groups. From 6.E.9 deduce that:

a) The order of G is a power of the prime number p if and only if order of every element of G is a power of p. (A group in which all elements are of order p^m, p prime, $m \in \mathbb{N}$, is called a <u>p-group</u>.)

b) Every subgroup of the product group $G \times H$ is of the form $G' \times H'$, where G' is a subgroup of G and H' is a subgroup of H, if and only if the orders of G and H are relatively prime.

10 If G is a finite group of odd order, and $a \in G$, $a \neq e_G$, then show that a and a^{-1} belong to the different conjugacy classes in G.

11 Let V be an n-dimensional K-vector space and let $G := \mathrm{Aut}_K V = GL_K V$ be the automorphism group of V. Then (with the natural operation of G on V)

a) G operates transitively on $V \setminus \{0\}$.

b) G operates simply transitively on the set of basis tuples $(v_1, \cdots, v_n)$ of V.

c) G operates transitively on the set of all r-dimensional subspaces of V, $r \leq n$.

d) G operates transitively on the set of flags: $0 = V_0 \subsetneqq V_1 \subsetneqq \cdots \subsetneqq V_n = V$ of V.

e) G operates (canonically) on V^* and transitively on $V^* \setminus \{0\}$. The corresponding group homomorphism

$$G \longrightarrow \mathfrak{S}(V^*)$$

is the well-known contra-gradient representation $GL_K V \longrightarrow GL_K V^*$, $g \longmapsto (g^{-1})^* = (g^*)^{-1}$.

f) For operations in parts a) to e) compute the isotropy groups.

12 Let G be a finite group which operates on a finite set X. Then

$$\# G \cdot \# (X \backslash G) = \sum_{g \in G} \# \mathrm{Fix}_g X ,$$

where $\mathrm{Fix}_g X$ is the set of fixed-points of g (Burnside's Formula). (Hint: Consider the set $\{(g,x) \in G \times X \mid gx = x\} \subseteq G \times X$.)