$$\mathbb{x} = \begin{pmatrix} \boldsymbol{p} \\ \hline 1 \end{pmatrix} \in \mathbb{A}_n$$

can easily be found as

$$\mathbb{W}\mathbb{x} = \begin{pmatrix} \boldsymbol{W}\boldsymbol{p} + \boldsymbol{w} \\ \hline 1 \end{pmatrix}.$$

If one has a way to measure lengths and angles (*i.e.* a Euclidean metric) on the underlying vector space $\tau(\mathbb{A}_n)$, one can compute the *distance* between P and $Q \in \mathbb{A}_n$ as the length of the vector $\overrightarrow{PQ}$ and the angle determined by P, Q and $R \in \mathbb{A}_n$ with vertex Q is obtained from $\cos(P,Q,R) = \cos(\overrightarrow{QP}, \overrightarrow{QR})$. In this case, $\mathbb{A}_n$ is the *Euclidean affine space*, $\mathbb{E}_n$.

An affine mapping of the Euclidean affine space is called an *isometry* if its linear part is an orthogonal mapping of the Euclidean space $\tau(\mathbb{A}_n)$. The set of all isometries in $\mathcal{A}_n$ is called the *Euclidean group* and denoted by $\mathcal{E}_n$. Hence $\mathcal{E}_n$ is the set of all distance-preserving mappings of $\mathbb{E}_n$ onto itself. The isometries are the affine mappings with matrices of the form

$$\mathbb{W} = \left(\begin{array}{c|c} \boldsymbol{W} & \boldsymbol{w} \\ \hline \boldsymbol{o}^{\mathrm{T}} & 1 \end{array}\right),$$

where the linear part $\boldsymbol{W}$ belongs to the orthogonal group of $\tau(\mathbb{A}_n)$.

Special isometries are the *translations*, the isometries where the linear part is $\boldsymbol{I}$, with matrix

$$\mathbb{T}_{\boldsymbol{w}} = \left(\begin{array}{c|c} \boldsymbol{I} & \boldsymbol{w} \\ \hline \boldsymbol{o}^{\mathrm{T}} & 1 \end{array}\right).$$

The group of all translations in $\mathcal{E}_n$ is the *translation subgroup* of $\mathcal{E}_n$ and is denoted by $\mathcal{T}_n$. Note that composition of two translations means addition of the translation vectors and $\mathcal{T}_n$ is isomorphic to the translation vector space $\tau(\mathbb{E}_n)$.

1.5.3. Groups

1.5.3.1. *Groups*

The affine group is only one example of the more general concept of a group. The following axiomatic definition sometimes makes it easier to examine general properties of groups.

Definition 1.5.3.1.1. A *group* $(\mathcal{G}, \cdot)$ is a set $\mathcal{G}$ with a mapping $\cdot : \mathcal{G} \times \mathcal{G} \to \mathcal{G}; (g,h) \mapsto g \cdot h$, called the *composition law* or *multiplication* of $\mathcal{G}$, satisfying the following three axioms:

(i) $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ for all $g, h, k \in \mathcal{G}$ (associative law).

(ii) There is an element $e \in \mathcal{G}$ called the *unit element* of $\mathcal{G}$ with $e \cdot g = g \cdot e = g$ for all $g \in \mathcal{G}$.

(iii) For all $g \in \mathcal{G}$, there is an element $g^{-1} \in \mathcal{G}$, called the *inverse* of g, with $g \cdot g^{-1} = g^{-1} \cdot g = e$. □

Normally the symbol $\cdot$ is omitted, hence the product $g \cdot h$ is just written as gh and the set $\mathcal{G}$ is called a group.

One should note that in particular property (i), the associative law, of a group is something very natural if one thinks of group elements as mappings. Clearly the composition of mappings is associative. In general, one can think of groups as groups of mappings as explained in Section 1.5.3.2.

A subset of elements of a group $\mathcal{G}$ which themselves form a group is called a subgroup:

Definition 1.5.3.1.2. A non-empty subset $\emptyset \neq \mathcal{U} \subseteq \mathcal{G}$ is called a *subgroup* of $\mathcal{G}$ (abbreviated as $\mathcal{U} \leq \mathcal{G}$) if $g \cdot h^{-1} \in \mathcal{U}$ for all $g, h \in \mathcal{U}$. □

The affine group is an example of a group where $\cdot$ is given by the composition of mappings. The unit element $e \in \mathcal{A}_n$ is the identity mapping given by the matrix

$$\mathbb{I} = \left(\begin{array}{c|c} \boldsymbol{I} & \boldsymbol{o} \\ \hline \boldsymbol{o}^{\mathrm{T}} & 1 \end{array}\right),$$

which also represents the translation by the vector $\mathbf{o}$. The composition of two affine mappings is again an affine mapping and the inverse of an affine mapping $\mathbb{W}$ has matrix

$$\mathbb{W}^{-1} = \left(\begin{array}{c|c} \boldsymbol{W}^{-1} & -\boldsymbol{W}^{-1}\boldsymbol{w} \\ \hline \boldsymbol{o}^{\mathrm{T}} & 1 \end{array}\right).$$

Since the inverse of an isometry and the composition of two isometries are again isometries, the set of isometries $\mathcal{E}_n$ is a subgroup of the affine group $\mathcal{A}_n$. The translation subgroup $\mathcal{T}_n$ is a subgroup of $\mathcal{E}_n$.

Any vector space $\mathbf{V}_n$ is a group with the usual vector addition as composition law. Therefore $\tau(\mathbb{A}_n)$ is also a group.

Remarks

(i) For every group $\mathcal{G}$, the set $\{e\}$ consisting only of the unit element of $\mathcal{G}$ is a subgroup of $\mathcal{G}$ called the *trivial subgroup* $\mathcal{I} = \{e\}$.

(ii) If $\mathcal{U}$ is a subgroup of $\mathcal{V}$ and $\mathcal{V}$ is a subgroup of the group $\mathcal{G}$, then $\mathcal{U}$ is a subgroup of $\mathcal{G}$.

(iii) If $\mathcal{U}$ and $\mathcal{V}$ are subgroups of the group $\mathcal{G}$, then the intersection $\mathcal{U} \cap \mathcal{V}$ is also a subgroup of $\mathcal{G}$.

(iv) If $S \subseteq \mathcal{G}$ is a subset of the group $\mathcal{G}$, then the smallest subgroup of $\mathcal{G}$ containing S is denoted by

$$\langle S \rangle := \bigcap \{\mathcal{U} \leq \mathcal{G} \mid S \subseteq \mathcal{U}\}$$

and is called the *subgroup generated by* S. The elements of S are called the *generators* of this group. It is convenient not to list all the elements of a group $\mathcal{G}$ but just to give generators of $\mathcal{G}$ (this also applies to finite groups).

Example 1.5.3.1.3.

A well known group is the addition group of integers $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$ where $\cdot$ is normally denoted by $+$ and the unit element $e \in \mathbb{Z}$ is 0. The group $\mathbb{Z}$ is generated by $\{1\}$. Other generating sets are for example $\{-1\}$ or $\{2, 3\}$. Taking two integers $a, b \in \mathbb{Z}$ which are divisible by some fixed integer $p \in \mathbb{Z}$, then the sum $a + b$ and the addition inverses $-a$ and $-b$ are again divisible by p. Hence the set $p\mathbb{Z}$ of all integers divisible by p is a subgroup of $\mathbb{Z}$. It is generated by $\{p\}$.

Definition 1.5.3.1.4. The *order* $|\mathcal{G}|$ of a group $\mathcal{G}$ is the number of elements in the set $\mathcal{G}$. □

Most of the groups $\mathcal{G}$ in crystallography, for example $\mathbb{Z}$, $\mathbf{V}_n$, $\mathcal{A}_n$, have infinite order.

Groups that are generated by one element are called *cyclic*. The cyclic group of order n is called $\mathcal{C}yc_n$. (We prefer to use three letters to denote the mathematical names of frequently occurring groups, since the more common symbol $\mathcal{C}_n$ could possibly cause confusion with the Schoenflies symbol C_n.)

The group $\mathbf{V}_n$ is not generated by a finite set.

These two groups $\mathbb{Z}$ and $\mathbf{V}_n$ have the property that for all elements g and h in the group it holds that $g \cdot h = h \cdot g$. Hence these two groups are Abelian in the sense of the following:

Definition 1.5.3.1.5. The group $(\mathcal{G}, \cdot)$ is called *Abelian* if $g \cdot h = h \cdot g$ for all $g, h \in \mathcal{G}$. □

1.5.3.2. *Actions of groups on sets*

The affine group $\mathcal{A}_n$ is defined *via* its action on the affine space $\mathbb{A}_n$. In general, the greatest significance of groups is that they act on sets.

Definition 1.5.3.2.1. Let $\mathcal{G}$ be a group. A non-empty set M is called a (*left*) $\mathcal{G}$*-set* if there is a mapping $\cdot : \mathcal{G} \times M \to M$ satisfying the following conditions:

(i) $(gh) \cdot m = g \cdot (h \cdot m)$ for all $g, h \in \mathcal{G}$ and $m \in M$.
(ii) $e \cdot m = m$ for all $m \in M$.

If M is a $\mathcal{G}$-set, one also says that $\mathcal{G}$ acts on M. □

Example 1.5.3.2.2.

(*a*) The affine space $\mathbb{A}_n$ is a $\mathcal{G}$-set for the affine group $\mathcal{G} = \mathcal{A}_n$.
(*b*) $\tau(\mathbb{A}_n)$ is an $\mathcal{A}_n$-set, where $\mathcal{A}_n$ acts *via* the linear parts.
(*c*) $\tau(\mathbb{A}_n)$ is also a group and acts on $\mathbb{A}_n$ by translations $\mathbf{v} \cdot P := P + \mathbf{v}$ for $\mathbf{v} \in \tau(\mathbb{A}_n)$, $P \in \mathbb{A}_n$.
(*d*) If $\mathcal{U} \leq \mathcal{G}$ is a subgroup of the group $\mathcal{G}$, then $\mathcal{G}$ is a $\mathcal{U}$-set where $\cdot : \mathcal{U} \times \mathcal{G} \to \mathcal{G}$ is the usual composition law. In particular, each group $\mathcal{G}$ is a $\mathcal{G}$-set and hence every group $\mathcal{G}$ can be viewed as a group of mappings from $\mathcal{G}$ onto $\mathcal{G}$.

Definition 1.5.3.2.3. Let $\mathcal{G}$ be a group and M a $\mathcal{G}$-set. If $m \in M$, then the set $\mathcal{G} \cdot m := \{g \cdot m | g \in \mathcal{G}\}$ is called the *orbit* of m under $\mathcal{G}$.
The $\mathcal{G}$-set M is called *transitive* if $M = \mathcal{G} \cdot m$ for any $m \in M$ consists of a single orbit under $\mathcal{G}$.
If $m \in M$ then the *stabilizer of m in* $\mathcal{G}$ is $\mathrm{Stab}_{\mathcal{G}}(m) := \{g \in \mathcal{G} \mid g \cdot m = m\}$.
The *kernel* $\mathcal{K}$ *of the action* of $\mathcal{G}$ on M is the intersection of the stabilizers of all elements in M,

$$\mathcal{K} := \{g \in \mathcal{G} \mid g \cdot m = m \text{ for all } m \in M\}.$$

M is called a *faithful* $\mathcal{G}$-set and the action of $\mathcal{G}$ on M is also called *faithful* if the kernel of the action is trivial, $\mathcal{K} = \{e\}$. □

Remarks

(i) If $m_1, m_2 \in M$, then their orbits are either equal or disjoint. For if there is an element $g_1 \cdot m_1 = g_2 \cdot m_2$, then by the axioms of $\mathcal{G}$-sets $m_1 = em_1 = (g_1^{-1}g_1) \cdot m_1 = g_1^{-1} \cdot (g_1 \cdot m_1) = g_1^{-1} \cdot (g_2 \cdot m_2) = (g_1^{-1}g_2) \cdot m_2$, hence every element $g \cdot m_1$ in the orbit of m_1 is of the form $g \cdot (g_1^{-1}g_2 \cdot m_2) = (gg_1^{-1}g_2) \cdot m_2$ and therefore lies in the orbit of m_2. Hence the set of orbits gives a partition of M into disjoint sets. If M is a finite set, then its order is the sum of the lengths of the different orbits.
(ii) $\mathrm{Stab}_{\mathcal{G}}(m)$ is a subgroup of $\mathcal{G}$, since for $g_1, g_2 \in \mathrm{Stab}_{\mathcal{G}}(m)$, the product $(g_1 g_2^{-1}) \cdot m = g_1 \cdot (g_2^{-1} \cdot m) = g_1 \cdot m = m$.
(iii) If $m_1 = g \cdot m_2$, then $\mathrm{Stab}_{\mathcal{G}}(m_1) = g\ \mathrm{Stab}_{\mathcal{G}}(m_2)g^{-1} = \{ghg^{-1} \mid h \in \mathrm{Stab}_{\mathcal{G}}(m_2)\}$.

Example 1.5.3.2.4. (Example 1.5.3.2.2 *cont.*)

(*a*) $\mathbb{A}_n$ is a transitive $\mathcal{A}_n$-set. This is a mathematical expression of the fact that in point space no point is distinguished.
(*b*) The $\mathcal{A}_n$-set $\tau(\mathbb{A}_n)$ decomposes into two orbits $\{\mathbf{o}\}$ and $\{\mathbf{v} \in \tau(\mathbb{A}_n) \mid \mathbf{v} \neq \mathbf{o}\}$. The kernel of the action of $\mathcal{A}_n$ on $\tau(\mathbb{A}_n)$ is the translation subgroup $\mathcal{T}_n$.
(*c*) $\tau(\mathbb{A}_n)$ acts transitively on $\mathbb{A}_n$. The kernel of the action only consists of the zero vector $\mathbf{o}$.

We now introduce some terminology for groups which is nicely formulated using $\mathcal{G}$-sets.

Definition 1.5.3.2.5. The orbit of $g \in \mathcal{G}$ under the action of the subgroup $\mathcal{U} \leq \mathcal{G}$ is the *right coset* $\mathcal{U}g = \{ug \mid u \in \mathcal{U}\}$ (*cf. IT* A, Section 8.1.5). Analogously one defines a *left coset* as

$$g\mathcal{U} = \{gu \mid u \in \mathcal{U}\}$$

and denotes the set of left cosets by $\mathcal{G}/\mathcal{U}$.
If the number of left cosets (which is always equal to the number of right cosets) of $\mathcal{U}$ in $\mathcal{G}$ is finite, then this number is called the *index* $[\mathcal{G} : \mathcal{U}]$ of $\mathcal{U}$ in $\mathcal{G}$. If this number is infinite, one says that the index of $\mathcal{U}$ in $\mathcal{G}$ is infinite. □

Example 1.5.3.2.6.

$\mathbb{A}_n$ is a coset of $\mathbf{V}_n$ in $\mathbf{V}_{n+1}$, namely

$$\mathbb{A}_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \hline 1 \end{pmatrix} + \mathbf{V}_n.$$

If one thinks of $\mathbb{A}_2$ as an infinite sheet of paper and puts uncountably many such sheets of paper (one for each real number) one onto the other, one gets the whole 3-space $\mathbf{V}_3$.

Remark
The set of left cosets $\mathcal{G}/\mathcal{U}$ is a left $\mathcal{G}$-set with the operation $g \cdot (m\mathcal{U}) := (gm)\mathcal{U}$ for all $g, m \in \mathcal{G}$. The kernel of the action is the intersection of all subgroups of $\mathcal{G}$ that are conjugate to $\mathcal{U}$ and is called the *core* of $\mathcal{U}$: $\mathrm{core}(\mathcal{U}) := \bigcap_{g \in \mathcal{G}} g\mathcal{U}g^{-1}$.

We now assume that $|\mathcal{G}|$ is finite. Let $\mathcal{U} \leq \mathcal{G}$ be a subgroup of $\mathcal{G}$. Then the set $\mathcal{G}$ is partitioned into left cosets of $\mathcal{U}$, $\mathcal{G} = g_1\mathcal{U} \cup \ldots \cup g_i\mathcal{U}$, where $i = [\mathcal{G} : \mathcal{U}]$ is the index of $\mathcal{U}$ in $\mathcal{G}$. Since the orders of the left cosets of $\mathcal{U}$ are all equal to the order of $\mathcal{U}$, one gets

Theorem 1.5.3.2.7. (Theorem of Lagrange.) Let $\mathcal{U}$ be a subgroup of the finite group $\mathcal{G}$. Then

$$|\mathcal{G}| = |\mathcal{U}|[\mathcal{G} : \mathcal{U}].$$

In particular, the order of any subgroup of $\mathcal{G}$ and also the index of any subgroup of $\mathcal{G}$ are divisors of the group order $|\mathcal{G}|$. □

The $\mathcal{G}$-set $\mathcal{G}/\mathcal{U}$ is only a special case of a $\mathcal{G}$-set. It is a transitive $\mathcal{G}$-set. If $M = \mathcal{G} \cdot m$ is a transitive $\mathcal{G}$-set, then the mapping $M \to \mathcal{G}/\mathrm{Stab}_{\mathcal{G}}(m), g \cdot m \mapsto g\mathrm{Stab}_{\mathcal{G}}(m)$ is a bijection (in fact an isomorphism of $\mathcal{G}$-sets in the sense of Definition 1.5.3.4.1 below). Therefore the number of elements of M, which is the length of the orbit of m under $\mathcal{G}$, equals the index of the stabilizer of m in $\mathcal{G}$, whence one gets the following generalization of the theorem of Lagrange:

Theorem 1.5.3.2.8. Let $\mathcal{G}$ be a finite group and M be a $\mathcal{G}$-set. Then

$$|\mathcal{G}| = |\mathcal{G} \cdot m||\mathrm{Stab}_{\mathcal{G}}(m)|$$

for all $m \in M$. □

Up to now, we have only considered the action of $\mathcal{G}$ upon $\mathcal{G}$ *via* multiplication. There is another natural action of $\mathcal{G}$ on itself *via conjugation*: $\mathcal{G} \times \mathcal{G} \to \mathcal{G}$ defined by $g \cdot m := gmg^{-1}$ for all group elements g and elements m in the $\mathcal{G}$-set $\mathcal{G}$. The stabilizer of m is called the *centralizer* of m in $\mathcal{G}$,

$$\mathrm{Stab}_{\mathcal{G}}(m) = \mathcal{C}_{\mathcal{G}}(m) = \{g \in \mathcal{G} \mid gmg^{-1} = m\}.$$

If $M \subset \mathcal{G}$ is a set of group elements, then the *centralizer of M* is the intersection of the centralizers of the elements in M:

$$\mathcal{C}_{\mathcal{G}}(M) = \{g \in \mathcal{G} \mid gmg^{-1} = m \text{ for all } m \in M\}.$$

Definition 1.5.3.2.9. $\mathcal{G}$ also acts on the set $\mathbf{U}$ of all subgroups of $\mathcal{G}$ by conjugation, $g \cdot \mathcal{U} := g\mathcal{U}g^{-1}$. The stabilizer of an element $\mathcal{U} \in \mathbf{U}$ is called the *normalizer of* $\mathcal{U}$ and denoted by $\mathcal{N}_{\mathcal{G}}(\mathcal{U})$. $\mathcal{U}$ is called a *normal subgroup of* $\mathcal{G}$ (denoted as $\mathcal{U} \trianglelefteq \mathcal{G}$) if $\mathcal{N}_{\mathcal{G}}(\mathcal{U}) = \mathcal{G}$. □

Remarks

(i) Let $\mathcal{U} \leq \mathcal{G}$. Then the index of the normalizer in $\mathcal{G}$ of $\mathcal{U}$ is the number of subgroups of $\mathcal{G}$ that are conjugate to $\mathcal{U}$. Since $\mathcal{U}$ always normalizes itself [hence $\mathcal{U}$ is a subgroup of $\mathcal{N}_{\mathcal{G}}(\mathcal{U})$], the index of the normalizer divides the index of $\mathcal{U}$.

(ii) If $\mathcal{G}$ is Abelian, then the conjugation action of $\mathcal{G}$ is trivial, hence each subgroup of $\mathcal{G}$ is a normal subgroup.

(iii) The group $\mathcal{G}$ itself and also the trivial subgroup $\{e\} \leq \mathcal{G}$ are always normal subgroups of $\mathcal{G}$.

Normal subgroups play an important role in the investigation of groups. If $\mathcal{N} \trianglelefteq \mathcal{G}$ is a normal subgroup, then the left coset $g\mathcal{N}$ equals the right coset $\mathcal{N}g$ for all $g \in \mathcal{G}$, because $g\mathcal{N} = g(g^{-1}\mathcal{N}g) = \mathcal{N}g$.

The most important property of normal subgroups is that the set of left cosets of $\mathcal{N}$ in $\mathcal{G}$ forms a group, called the *factor group* $\mathcal{G}/\mathcal{N}$, as follows: The set of all products of elements of two left cosets of $\mathcal{N}$ again forms a left coset of $\mathcal{N}$. Let $g, h \in \mathcal{G}$. Then

$$g\mathcal{N}h\mathcal{N} = g(h\mathcal{N}h^{-1})h\mathcal{N} = gh\mathcal{N}\mathcal{N} = gh\mathcal{N}.$$

This defines a natural product on the set of left cosets of $\mathcal{N}$ in $\mathcal{G}$ which turns this set into a group. The unit element is $e\mathcal{N}$.

Hence the philosophy of normal subgroups is that they cut the group into pieces, where the two pieces $\mathcal{G}/\mathcal{N}$ and $\mathcal{N}$ are again groups.

Example 1.5.3.2.10.

The group $\mathbb{Z}$ is Abelian. For any number $p \in \mathbb{Z}$, the set $p\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Hence $p\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. The factor group $\mathbb{Z}/p\mathbb{Z}$ inherits the multiplication from the multiplication in $\mathbb{Z}$, since $ap\mathbb{Z} \subset p\mathbb{Z}$ for all $a \in \mathbb{Z}$. If p is a prime number, then all elements $\neq 0 + p\mathbb{Z}$ in $\mathbb{Z}/p\mathbb{Z}$ have a multiplicative inverse, and therefore $\mathbb{Z}/p\mathbb{Z}$ is a field, the *field with p elements*.

Proposition 1.5.3.2.11.
Let $\mathcal{N} \trianglelefteq \mathcal{G}$ be a normal subgroup of the group $\mathcal{G}$ and $\mathcal{U} \leq \mathcal{G}$. Then the set

$$\mathcal{N}\mathcal{U} = \mathcal{U}\mathcal{N} := \{un \mid u \in \mathcal{U}, n \in \mathcal{N}\}$$

is a subgroup of $\mathcal{G}$. □

Proof. Let $u_1n_1, u_2n_2 \in \mathcal{U}\mathcal{N}$. Then $u_1n_1(u_2n_2)^{-1} = u_1n_1n_2^{-1}u_2^{-1}$ $= un \in \mathcal{U}\mathcal{N}$, where $u := u_1u_2^{-1} \in \mathcal{U}$, since $\mathcal{U}$ is a subgroup of $\mathcal{G}$, and $n := u_2n_1n_2u_2^{-1} \in \mathcal{N}$, since $\mathcal{N}$ is a normal subgroup of $\mathcal{G}$. QED

1.5.3.3. *The Sylow theorems*

A nice application of the notion of $\mathcal{G}$-sets are the three theorems of Sylow. By Theorem 1.5.3.2.7, the order of any subgroup $\mathcal{U}$ of a group $\mathcal{G}$ divides the order of $\mathcal{G}$. But conversely, given a divisor d of $|\mathcal{G}|$, one cannot predict the existence of a subgroup $\mathcal{U}$ of $\mathcal{G}$ with $|\mathcal{U}| = d$. If $d = p^\beta$ is a prime power that divides $|\mathcal{G}|$, then the following theorem says that such a subgroup exists.

Theorem 1.5.3.3.1. (Sylow)
Let $\mathcal{G}$ be a finite group and p be a prime such that p^β divides the order of $\mathcal{G}$. Then $\mathcal{G}$ possesses m subgroups of order p^β, where $m > 0$ satisfies $m \equiv 1 \pmod{p}$. □

Theorem 1.5.3.3.2. (Sylow)
If $|\mathcal{G}| = p^\alpha s$ for some prime p not dividing s, then all subgroups of order p^α of $\mathcal{G}$ are conjugate in $\mathcal{G}$. Such a subgroup $\mathcal{U} \leq \mathcal{G}$ of order $|\mathcal{U}| = p^\alpha$ is called a *Sylow p-subgroup*. □

Combining these two theorems with Theorem 1.5.3.2.8, one gets Sylow's third theorem:

Theorem 1.5.3.3.3. (Sylow)
The number of Sylow p-subgroups of $\mathcal{G}$ is $\equiv 1 \pmod{p}$ and divides the order of $\mathcal{G}$. □

Proofs of the three theorems above can be found in Ledermann (1976), pp.158–164.

1.5.3.4. *Isomorphisms*

If one wants to compare objects such as groups or $\mathcal{G}$-sets, to be able to say when they should be considered as equal, the concept of isomorphisms should be used:

Definition 1.5.3.4.1. Let $\mathcal{G}$ and $\mathcal{H}$ be groups and M and N be $\mathcal{G}$-sets.

(*a*) A *homomorphism* $\varphi : \mathcal{G} \to \mathcal{H}$ is a mapping of the set $\mathcal{G}$ into the set $\mathcal{H}$ respecting the composition law *i.e.* $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in \mathcal{G}$.
If φ is bijective, it is called an *isomorphism* and one says $\mathcal{G}$ is *isomorphic* to $\mathcal{H}$ ($\mathcal{G} \cong \mathcal{H}$).
If $e \in \mathcal{H}$ is the unit element of $\mathcal{H}$, then the set of all pre-images of e is called the *kernel* of φ: $\ker(\varphi) := \{g \in \mathcal{G} \mid \varphi(g) = e\}$.
An isomorphism $\varphi : \mathcal{G} \to \mathcal{G}$ is called an *automorphism* of $\mathcal{G}$.

(*b*) M and N are called *isomorphic* $\mathcal{G}$-sets if there is a bijection $\varphi : M \to N$ with $g \cdot \varphi(m) = \varphi(g \cdot m)$ for all $g \in \mathcal{G}, m \in M$. □

Example 1.5.3.4.2.

In Example 1.5.3.1.3, the group homomorphism $\mathbb{Z} \to p\mathbb{Z}$ defined by $1 \mapsto p$ is a group isomorphism (from the group $\mathbb{Z}$ onto its subgroup $p\mathbb{Z}$).

Example 1.5.3.4.3.

For any group element $g \in \mathcal{G}$, conjugation by g defines an automorphism of $\mathcal{G}$. In particular, if $\mathcal{U}$ is a subgroup of $\mathcal{G}$, then $\mathcal{U}$ and its conjugate subgroup $g\mathcal{U}g^{-1}$ are isomorphic.

Philosophy: If $\mathcal{G}$ and $\mathcal{H}$ are isomorphic groups, then all group-theoretical properties of $\mathcal{G}$ and $\mathcal{H}$ are the same. The calculations in $\mathcal{G}$ can be translated by the isomorphism to calculations in $\mathcal{H}$. Sometimes it is easier to calculate in one group than in the other and translate the result back *via* the inverse of the isomorphism. For example, the isomorphism between $\tau(\mathbb{A}_n)$ and $\mathbf{V}_n$ in Section 1.5.2 is an isomorphism of groups. It even respects scalar multiplication with real numbers, so in fact it is an isomorphism of vector spaces. While the composition of translations is more concrete and easier to imagine, the calculation of the resulting vector is much easier in $\mathbf{V}_n$. The concept of isomorphism says that you can translate to the more convenient group for your calculations and translate back afterwards without losing anything.

Note that a homomorphism is injective, *i.e.* is an isomorphism onto its image, if and only if its kernel is trivial ($= \{e\}$).

Example 1.5.3.4.4.

The mapping

$$\mu : \tau(\mathbb{A}_n) \to \mathcal{A}_n, \boldsymbol{w} \mapsto \left(\begin{array}{c|c} \boldsymbol{I} & \boldsymbol{w} \\ \hline \boldsymbol{o}^{\mathrm{T}} & 1 \end{array}\right)$$

is a homomorphism of the group $\tau(\mathbb{A}_n)$ into $\mathcal{A}_n$. The kernel of this homomorphism is $\{\boldsymbol{o}\}$ and the image of the mapping is the

translation subgroup $\mathcal{T}_n$ of $\mathcal{A}_n$. Hence the groups $\tau(\mathbb{A}_n)$ and $\mathcal{T}_n$ are isomorphic.

The affine group acts (as group of group automorphisms) on the normal subgroup $\mathcal{T}_n \trianglelefteq \mathcal{A}_n$ *via* conjugation: $g \cdot t := gtg^{-1}$. We have seen already in Example 1.5.3.2.4 (*b*) that it also acts (as a group of linear mappings) on $\tau(\mathbb{A}_n)$. The mapping μ is an isomorphism of $\mathcal{A}_n$-sets.

1.5.3.5. *Isomorphism theorems*

[*cf.* Ledermann (1976), pp. 68–73.]

Remark
If φ is a homomorphism $\mathcal{G} \to \mathcal{H}$ and $\mathcal{N} \trianglelefteq \mathcal{H}$ is a normal subgroup of $\mathcal{H}$, then the pre-image $\varphi^{-1}(\mathcal{N}) := \{g \in \mathcal{G} \mid \varphi(g) \in \mathcal{N}\}$ is a normal subgroup of $\mathcal{G}$. In particular, it holds that $\ker(\varphi) \trianglelefteq \mathcal{G}$.

Hence the factor group $\mathcal{G}/\ker(\varphi)$ is a well defined group. The following theorem says that this group is isomorphic to the image $\varphi(\mathcal{G}) \leq \mathcal{H}$ of φ:

Theorem 1.5.3.5.1. (First isomorphism theorem.)
Let $\varphi : \mathcal{G} \to \mathcal{H}$ be a homomorphism of groups. Then

$$\overline{\varphi} : \mathcal{G}/\ker(\varphi) \to \varphi(\mathcal{G}) \leq \mathcal{H}.$$

$g\ker(\varphi) \mapsto \varphi(g)$ is an isomorphism between the factor group $\mathcal{G}/\ker(\varphi)$ and the image group of φ, which is a subgroup of $\mathcal{H}$. □

Theorem 1.5.3.5.2. (Third isomorphism theorem.)
Let $\mathcal{N} \trianglelefteq \mathcal{G}$ be a normal subgroup of the group $\mathcal{G}$ and $\mathcal{U} \leq \mathcal{G}$ be an arbitrary subgroup of $\mathcal{G}$. Then $\mathcal{U} \cap \mathcal{N} \trianglelefteq \mathcal{U}$ is a normal subgroup of $\mathcal{U}$ and

$$\mathcal{U}/(\mathcal{U} \cap \mathcal{N}) \cong \mathcal{N}\mathcal{U}/\mathcal{N}.$$

(For the definition of the group $\mathcal{N}\mathcal{U}$ see Proposition 1.5.3.2.11.) □

Definition 1.5.3.5.3. A subgroup $\mathcal{U} \leq \mathcal{H}$ is a *characteristic subgroup* $\mathcal{U}$ char $\mathcal{H}$ if $\varphi(\mathcal{U}) = \mathcal{U}$ for all automorphisms φ of $\mathcal{H}$. □

Remarks

(*a*) If $\mathcal{H}$ is a finite Abelian group and $\mathcal{P}$ is a Sylow p-subgroup of $\mathcal{H}$, then $\mathcal{P}$ char $\mathcal{H}$, because $\mathcal{P}$ is the only subgroup of $\mathcal{H}$ of order $|\mathcal{P}|$.

(*b*) If $\mathcal{H}$ is any group and $\mathcal{U}$ char $\mathcal{H}$, then $\mathcal{U} \trianglelefteq \mathcal{H}$ is also a normal subgroup of $\mathcal{H}$: for $h \in \mathcal{H}$ define the mapping $\kappa_h : \mathcal{H} \to \mathcal{H}, x \mapsto hxh^{-1}$. Then κ_h is an automorphism of $\mathcal{H}$ and $\kappa_h(\mathcal{U}) = h\mathcal{U}h^{-1} = \mathcal{U}$ since $\mathcal{U}$ is characteristic in $\mathcal{H}$.

(*c*) If $\mathcal{U}$ char $\mathcal{N} \trianglelefteq \mathcal{H}$, then $\mathcal{U} \trianglelefteq \mathcal{H}$, since the conjugation with any element of $\mathcal{H}$ induces an automorphism of $\mathcal{N}$.

1.5.3.6. *An example*

Let us consider the tetrahedral group, Schoenflies symbol T_d, which is defined as the symmetry group of a tetrahedron. It permutes the four apices P_1, P_2, P_3, P_4 of the tetrahedron and hence every element of T_d defines a bijection of $V := \{P_1, P_2, P_3, P_4\}$ onto itself. The only element that fixes all the apices is e. Therefore the set V is a faithful T_d-set. Let us calculate the order of $|T_d|$. Since there are elements in T_d that map the first apex P_1 onto each one of the other apices, V is a transitive T_d-set. Let $\mathcal{S} := \mathrm{Stab}_{T_d}(P_1)$ be the stabilizer of P_1. By Theorem 1.5.3.2.8, $|T_d| = |V||\mathcal{S}| = 4|\mathcal{S}|$. The group $\mathcal{S}$ is generated by the threefold rotation r around the 'diagonal' of the tetrahedron through P_1 and the reflection s at the symmetry plane of the tetrahedron which contains the edge (P_1, P_2). In particular, $\mathcal{S}$ acts transitively on the set $\{P_2, P_3, P_4\}$. The stabilizer of P_2 in $\mathcal{S}$ is the cyclic group $\langle s \rangle \cong \mathcal{C}yc_2$ generated by s. (The Schoenflies notation for $\langle s \rangle$ is C_s and the Hermann–Mauguin symbol is m.) Therefore $|\mathcal{S}| = 3|\langle s \rangle| = 6$ and $|T_d| = 24$. In fact, we have seen that T_d is isomorphic to the group of all bijections of V onto itself, which is the symmetric group $\mathcal{S}ym_4$ of degree 4 and the group $\mathcal{S} \cong \mathcal{S}ym_3$ is the symmetric group on $\{P_2, P_3, P_4\}$. The Schoenflies notation for $\mathcal{S}$ is C_{3v} and its Hermann–Mauguin symbol is $3m$.

In general, let $n \in \mathbb{N}$ be a natural number. Then the group of all bijective mappings of the set $\{1, \ldots, n\}$ onto itself is called the *symmetric group of degree n* and denoted by

$$\mathcal{S}ym_n := \{f : \{1, \ldots, n\} \to \{1, \ldots, n\} \mid f \text{ is bijective}\}.$$

The *alternating group* is the normal subgroup $\mathcal{A}lt_n$ consisting of all even permutations of $\{1, \ldots, n\}$.

Let us construct a normal subgroup of T_d. The tetrahedral group contains three twofold rotations r_1, r_2, r_3 around the three axes of the tetrahedron through the midpoints of opposite edges. Since T_d permutes these three axes and hence conjugates the three rotations into each other, the group

$$\mathcal{U} := \langle r_1, r_2, r_3 \rangle$$

generated by these three rotations is a normal subgroup of T_d. Since these three rotations commute with each other, the group $\mathcal{U}$ is Abelian. Now $r_1 r_2 = r_3$ and hence $\mathcal{U} = \{e, r_1, r_2, r_3\} \cong D_2$ (in Schoenflies notation) $\cong 222$ (Hermann–Mauguin symbol) is of order 4. There are three normal subgroups of order 2 in $\mathcal{U}$, namely $\langle r_i \rangle$ for $i = 1, 2, 3$. The factor group $\mathcal{U}/\langle r_1 \rangle$ is again of order 2. Since all groups of order 2 are cyclic, $\langle r_1 \rangle \cong \mathcal{U}/\langle r_1 \rangle \cong \mathcal{C}yc_2$. The set $\mathcal{U}$ is the set of all products of elements from the two normal subgroups $\langle r_1 \rangle$ and $\langle r_2 \rangle$, hence $\mathcal{U}$ is isomorphic to the *direct product* $\mathcal{C}yc_2 \times \mathcal{C}yc_2$ in the sense of the following definition.

Definition 1.5.3.6.1. [*cf.* Ledermann (1976), Section 13.] Let $\mathcal{G}$ and $\mathcal{H}$ be two groups. Then the *direct product* $\mathcal{G} \times \mathcal{H}$ is the group $\mathcal{G} \times \mathcal{H} = \{(g, h) \mid g \in \mathcal{G}, h \in \mathcal{H}\}$ with multiplication $(g, h)(g', h') := (gg', hh')$. □

Let us return to the example above. The centralizer of one of the three rotations, say of r_1, is of index 3 in T_d and hence a Sylow 2-subgroup of T_d with order 8. Following Schoenflies, we will denote this group by D_{2d} (another Schoenflies symbol for this group is S_{4v} and its Hermann–Mauguin symbol is $\bar{4}2m$).

The group $\mathcal{U}$ above is contained in D_{2d}. It is its own centralizer in T_d: $\mathcal{U} = \mathcal{C}_{T_d}(\mathcal{U})$. Therefore the factor group $T_d/\mathcal{U}$ acts faithfully (and transitively) on the set $\{r_1, r_2, r_3\}$. The stabilizer of r_1 is the subgroup D_{2d} constructed above. Using this, one easily sees that $T_d/\mathcal{U} \cong \mathcal{S}ym_3$.

Another normal subgroup in T_d is the set of all rotations in T_d. This group contains the normal subgroup $\mathcal{U}$ above of index 3 and is of index 2 in T_d (and hence has order 12). It is isomorphic to $\mathcal{A}lt_4$, the alternating group of degree 4, and has Schoenflies symbol T and Hermann–Mauguin symbol 23.

1.5.4. Space groups

1.5.4.1. *Definition of space groups*

In *IT* A (2002), Section 8.1.6, space groups are introduced as symmetry groups of crystal patterns.

references