International Tables for Crystallography (2011). Vol. A1, Section 1.4.3.2, pp. 30–31.

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 1.4.3.1.3

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 negatives $-a$ 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 1.4.3.1.4. 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 1.4.3.1.5. The group $(\mathcal{G}, \cdot)$ is called *Abelian* if $g \cdot h = h \cdot g$ for all $g, h \in \mathcal{G}$. □

1.4.3.2. 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 1.4.3.2.1. Let $\mathcal{G}$ be a group. A non-empty set M is called a (*left*) $\mathcal{G}$*-set* if there is a mapping $\mathcal{G} \times M \to M$ 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 1.4.3.2.2

(*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 $\mathcal{U} \le \mathcal{G}$ 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 1.4.3.2.3. 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 $\mathrm{Stab}_{\mathcal{G}}(m) := \{g \in \mathcal{G} \mid g \cdot m = m\}$.

For a space group $\mathcal{G}$ and a point P in the point space, the stabilizer $\mathrm{Stab}_{\mathcal{G}}(P)$ is called the *site-symmetry group* of P with respect to $\mathcal{G}$.

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, $\mathcal{K} = \{e\}$. □

Note that any space group $\mathcal{R}$ acts faithfully on the point space.

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 $(g_1g_2^{-1}) \cdot m = g_1 \cdot (g_2^{-1} \cdot m) = g_1 \cdot m = m$.
(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 1.4.3.2.4 (Example 1.4.3.2.2 continued)

(*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 $\{\mathbf{v} \in \tau(\mathbb{A}_n) \mid \mathbf{v} \ne \mathbf{o}\}$. 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 1.4.3.2.5. The orbit of $g \in \mathcal{G}$ under the action of the subgroup $\mathcal{U} \le \mathcal{G}$ 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 1.4.3.2.6

$\mathbb{A}_n$ 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 $\mathcal{U}$: 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 1.4.3.2.7. (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 1.4.3.4.1 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 1.4.3.2.8. 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 $m \in M$. □

The point group $\mathcal{G}$ acts on the finite set M of ideal crystal faces. Then the length of the orbit (the number of equivalent crystal faces) times the order of the face-symmetry group is the order of the point group.

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 1.4.3.2.9. $\mathcal{G}$ 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 of $\mathcal{U}$ in $\mathcal{G}$ 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 1.4.3.2.10. 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 1.4.3.2.11. 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

$$u_1n_1(u_2n_2)^{-1} = u_1n_1n_2^{-1}u_2^{-1} = u_1u_2^{-1}(u_2n_1n_2^{-1}u_2^{-1}) = un \in \mathcal{U}\mathcal{N},$$

where $u := u_1u_2^{-1} \in \mathcal{U}$, since $\mathcal{U}$ is a subgroup of $\mathcal{G}$, and $n := u_2n_1n_2^{-1}u_2^{-1} \in \mathcal{N}$, since $\mathcal{N}$ is a normal subgroup of $\mathcal{G}$. QED

1.4.3.3. The Sylow theorems

A nice application of the notion of $\mathcal{G}$-sets are the three theorems of Sylow. By Theorem 1.4.3.2.7, 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 1.4.3.3.1. (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 $m \equiv 1 \pmod{p}$. □

In particular this theorem implies that for every prime power that divides the order of the finite group $\mathcal{G}$, the group $\mathcal{G}$ has a subgroup whose order is this prime power. This is not true for composite numbers. For instance, the alternating group $\mathcal{A}lt_4$ of order 12 (Hermann–Mauguin notation 23) has no subgroup of order 6. This group has three subgroups of order 2, a unique subgroup of order 4 = 2^2 and four subgroups of order 3. The group $\mathcal{C}yc_2 \times \mathcal{S}ym_3$ (Hermann–Mauguin notation $\bar{3}m$) also has order 12 but seven subgroups of order 2, three subgroups of order 4 and a unique subgroup of order 3.

references