*International Tables for Crystallography* (2011). Vol. A1, Section 1.4.3.3, pp. 31–32.



*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 $\mathcal{U} \le \mathcal{G}$ 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 $\mathcal{U} \le \mathcal{G}$. 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 $\{e\} \le \mathcal{G}$ 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 $\mathcal{U} \le \mathcal{G}$. 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 $p^{\beta}$ divides the order of $\mathcal{G}$. Then $\mathcal{G}$ possesses $m$ subgroups of order $p^{\beta}$, 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.

**Theorem 1.4.3.3.2.** (Sylow) If $|\mathcal{G}| = p^\alpha s$ for some prime $p$ not dividing $s$, then all subgroups of order $p^\alpha$ 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 1.4.3.2.8, one gets Sylow's third theorem:

**Theorem 1.4.3.3.3.** (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, or in Ledermann & Weir (1996), pp. 155–161.

*1.4.3.4. Isomorphisms*

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

**Definition 1.4.3.4.1.** 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 $\varphi$ 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 $\varphi$: $\ker(\varphi) := \{g \in \mathcal{G} \mid \varphi(g) = e\}$. 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 1.4.3.4.2.* In Example 1.4.3.1.3, 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 1.4.3.4.3.* 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 1.4.2 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, hence an isomorphism onto its image, if and only if its kernel is trivial ($= \{e\}$).

*Example 1.4.3.4.4*

The mapping $\mu$ from the space $\tau(\mathbb{A}_n)$ of translation vectors into the affine group $\mathcal{A}_n$ defined by

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

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 1.4.3.2.4 (*b*) that it also acts (as a group of linear mappings) on $\tau(\mathbb{A}_n)$. The mapping $\mu$ is an isomorphism of $\mathcal{A}_n$-sets.

*1.4.3.5. Isomorphism theorems*

[*cf.* Ledermann (1976), pp. 68–73, or Ledermann & Weir (1996), pp. 85–92.]

*Remark*. If $\varphi$ 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 $\varphi$:

**Theorem 1.4.3.5.1.** (First isomorphism theorem.) Let $\varphi : \mathcal{G} \to \mathcal{H}$ be a homomorphism of groups. Then

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

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

For instance, if $\mathcal{R}$ is a space group and $\varphi$ is mapping any element

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

to its linear part $\boldsymbol{W}$, then the kernel of $\varphi$ is the translation group $\mathcal{T}(\mathcal{R})$ of $\mathcal{R}$ and the image is the point group $\overline{\mathcal{R}}$ of $\mathcal{R}$. The theorem says that the point group $\overline{\mathcal{R}}$ is isomorphic to the factor group $\mathcal{R}/\mathcal{T}(\mathcal{R})$.

**Theorem 1.4.3.5.2.** (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 1.4.3.2.11.) □

**Definition 1.4.3.5.3.** A subgroup $\mathcal{U} \leq \mathcal{H}$ is a *characteristic subgroup* $\mathcal{U} \operatorname{char} \mathcal{H}$ if $\varphi(\mathcal{U}) = \mathcal{U}$ for all automorphisms $\varphi$ 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 $\mathcal{P} \operatorname{char} \mathcal{H}$, because $\mathcal{P}$ is the only subgroup of $\mathcal{H}$ of order $|\mathcal{P}|$.

(*b*) If $\mathcal{H}$ is any group and $\mathcal{U} \operatorname{char} \mathcal{H}$, 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 $\kappa_h$ is an automorphism of $\mathcal{H}$ and $\kappa_h(\mathcal{U}) = h\mathcal{U}h^{-1} = \mathcal{U}$ since $\mathcal{U}$ is characteristic in $\mathcal{H}$.


references