3. Subgroups and complexes

If a subset $\mathcal{H}$ of elements of a group $\mathcal{G}$ is itself a group (under the same rule of multiplication), then it is said to be a *subgroup* of $\mathcal{G}$, written $\mathcal{H} < \mathcal{G}$. It must contain the identity element of $\mathcal{G}$. Any finite subset $\mathcal{H}$ of a group $\mathcal{G}$ is a subgroup if and only if it is closed under multiplication.

[It automatically satisfies associativity, since it belongs to $\mathcal{G}$, and it has the cancellation property, for the same reason.]

From this it follows that the intersection of any number of subgroups is itself a subgroup. Both the group $\mathcal{G}$ itself and the trivial unit group consisting of the identity alone are subgroups of $\mathcal{G}$. They are known as *improper subgroups*. Any other subgroup is a *proper subgroup*.

A useful notion is the *complex*. This is a set of elements of the group, treated as a collection and with no duplicates. A complex may be multiplied by any element of the group, producing another complex — just the set of products of the chosen element with all the elements of the complex. (To be explicit, if $\{A_1, A_2, \ldots, A_m\}$ is a complex $\mathcal{A}$, then $B\mathcal{A} = \{BA_1, BA_2, \ldots, BA_m\}$ and $\mathcal{A}B = \{A_1B, A_2B, \ldots, A_mB\}$.) Two complexes may be multiplied together to produce a complex containing all pairwise products of members of the two complexes, omitting duplicates. (Note that the order of multiplication, left or right, is generally significant.) From now on, products of groups or subgroups, or products of elements with groups or subgroups, should be interpreted as products in the sense of complexes.

In terms of complexes, if $\mathcal{H} \subset \mathcal{G}$, then $\mathcal{H} < \mathcal{G} \iff \mathcal{H}^2 = \mathcal{H}$.

[**Proof:** (1) Suppose $\mathcal{H} < \mathcal{G}$. Then, by closure, $\mathcal{H}^2 \subset \mathcal{H}$. But since $\mathcal{H}$ contains the identity E, $\mathcal{H}^2 \supset \mathcal{H}$. So $\mathcal{H}^2 = \mathcal{H}$. (2) Suppose $\mathcal{H}^2 = \mathcal{H}$. Then the product of any two elements of $\mathcal{H}$ is in $\mathcal{H}$, i.e. $\mathcal{H}$ is closed under multiplication and so $\mathcal{H} < \mathcal{G}$.]

As an example of the utility of the "complex" notation, note that $\mathcal{H} < \mathcal{G} \Longrightarrow X\mathcal{H}X^{-1} < \mathcal{G}$ for any $X \in \mathcal{G}$.

$[(X\mathcal{H}X^{-1})^2 = X\mathcal{H}X^{-1}X\mathcal{H}X^{-1} = X(\mathcal{H})^2X^{-1} = X\mathcal{H}X^{-1}.]$

In fact, the two subgroups $\mathcal{H}$ and $X\mathcal{H}X^{-1}$ are isomorphic to one another under the natural mapping $(A \in \mathcal{H}) \to XAX^{-1}$.

In "complex" notation, the rearrangement theorem states that $X\mathcal{G} = \mathcal{G}$ for any $X \in \mathcal{G}$.

Suppose $\mathcal{H} < \mathcal{G}$, of orders $|\mathcal{H}| = h$ and $|\mathcal{G}| = g$. For any $A \in \mathcal{G}$, the complex $A\mathcal{H}$ contains h distinct elements, including A itself. It is called a

left coset of $\mathcal{G}$ relative to $\mathcal{H}$. (The complex $\mathcal{H}A$, also containing h distinct elements, including A, is called a *right coset* and is generally different from $A\mathcal{H}$.) Any element of a coset will generate the same coset, i.e. $B \in A\mathcal{H} \Longrightarrow B\mathcal{H} = A\mathcal{H}$.

> [$B \in A\mathcal{H} \Longrightarrow B = AH$, for some $H \in \mathcal{H}$, so $B\mathcal{H} = AH\mathcal{H} = A\mathcal{H}$, by the rearrangement theorem.]

Consider an element $B \in \mathcal{G}$ which does not belong to $A\mathcal{H}$. The left coset $B\mathcal{H}$ is completely distinct from $A\mathcal{H}$.

> [If some element of $B\mathcal{H}$ is also in $A\mathcal{H}$, then there are elements $H_1, H_2 \in \mathcal{H}$ such that $BH_1 = AH_2 \Longrightarrow B = AH_2H_1^{-1} \Longrightarrow B \in A\mathcal{H}$, since $H_2H_1^{-1} \in \mathcal{H}$ — a contradiction.]

Belonging to the same left coset is an equivalence relation, so the left cosets partition the group and each of them contains exactly h distinct elements. Suppose there are n such cosets. This is called the *index* of the subgroup $\mathcal{H}$ in the group $\mathcal{G}$. The above discussion shows that $g = nh$, which is known as *Lagrange's theorem*. From this it follows that the order of any subgroup exactly divides the order of the group. Note that the same discussion could have been carried through with right cosets, with the same index n.

The set of distinct powers of any element of a group is always closed under multiplication, so it is a (cyclic) subgroup of the group. Its order is the order of the element, so it may be concluded that the order of every element of the group necessarily divides the order of the group. (This is clearly true of the examples previously described.) Since only the identity element of a group has order 1, every non-identity element of a group of prime order has the same order as the group. Such a group has no proper subgroups and must be cyclic. It may fairly easily be proved that every subgroup of a cyclic group is cyclic, with one and only one subgroup of order h for every divisor h of g, and that every group of composite (not prime) order has proper subgroups.

Suppose $A \in \mathcal{G}$. The set of elements of $\mathcal{G}$ which commute with A is called the *normalizer* of A, denoted $\mathcal{N}_A$, and is of order n_A. Every element of a group commutes with itself and with the identity, so $n_A \geq 2$. If the order of the element is greater than 2, then the element commutes also with its inverse and $n_A \geq 3$. (An element of order 2 is its own inverse, since $A^2 = E$.) Since it is clearly closed under multiplication, $\mathcal{N}_A < \mathcal{G}$ and so n_A divides g and $h_A = g/n_A$ is the index of $\mathcal{N}_A$ in $\mathcal{G}$. An element and its inverse have the same normalizer.

$[X \in \mathcal{N}_A \iff XA = AX \iff A^{-1}XAA^{-1} = A^{-1}AXA^{-1} \iff A^{-1}X = XA^{-1} \iff X \in \mathcal{N}_{A^{-1}}.]$

Consider the coset decomposition of $\mathcal{G}$ relative to $\mathcal{N}_A$, say $\{T_i\mathcal{N}_A\}$, where the $T_i \in \mathcal{G}$, with $i = 1, 2, \ldots, h_A$, are representative elements of each of the cosets. For any $X \in \mathcal{N}_A$, the conjugate $(T_iX)A(T_iX)^{-1} = T_i(XAX^{-1})T_i^{-1} = T_iAT_i^{-1}$ (since X commutes with A), so all the elements of a given coset produce the same conjugate element of A. Two distinct cosets cannot generate the same conjugate element of A

$[\text{since } T_iAT_i^{-1} = T_jAT_j^{-1} \implies T_j^{-1}T_iA = AT_j^{-1}T_i \implies T_j^{-1}T_i \in \mathcal{N}_A \implies T_j^{-1}T_i\mathcal{N}_A = \mathcal{N}_A \implies T_i\mathcal{N}_A = T_j\mathcal{N}_A]$

so the number of distinct conjugates of A is h_A, the number of cosets in the decomposition relative to $\mathcal{N}_A$. The number of elements in the class generated by A is equal to the index of the normalizer of A and divides the order g of the group $\mathcal{G}$. It cannot exceed $g/2$ ($g/3$ if the order of A is greater than 2).

If $h_A = 1$ for some element $A \in \mathcal{G}$, then the class generated by A consists of the single element A alone. This A commutes with all the elements of $\mathcal{G}$ and is said to be a *self-conjugate*, or *invariant*, element. The identity element E is always invariant. The set of all self-conjugate elements of $\mathcal{G}$ is a subgroup of $\mathcal{G}$ (it is evidently closed under multiplication), called the *centre* of $\mathcal{G}$.

A subgroup $\mathcal{H} < \mathcal{G}$ which contains all the conjugates of all its elements is a self-conjugate subgroup. It satisfies $X\mathcal{H}X^{-1} = \mathcal{H}$, in the sense of complexes, for every $X \in \mathcal{G}$,

$[XH_iX^{-1} \in \mathcal{H} \text{ for every } H_i \in \mathcal{H} \text{ and } XH_iX^{-1} = XH_jX^{-1} \implies H_i = H_j]$

and is called an *invariant* or *normal* subgroup, denoted $\mathcal{H} \lhd \mathcal{G}$. A subgroup $\mathcal{H} < \mathcal{G}$ is invariant if and only if it contains only complete classes of elements of $\mathcal{G}$. For an invariant subgroup, the left and right cosets generated by a given element of $\mathcal{G}$ coincide.

$[H_i \in \mathcal{H}, X \in \mathcal{G} \implies XH_iX^{-1} = H_j \in \mathcal{H} \implies XH_i = H_jX.$ In terms of complexes, $X\mathcal{H}X^{-1} = \mathcal{H} \implies X\mathcal{H} = \mathcal{H}X.]$

In this case, the cosets form a group under multiplication of complexes

$[X_1\mathcal{H}X_2\mathcal{H} = X_1X_2\mathcal{H}^2 = X_1X_2\mathcal{H}$ (closure), the identity is $\mathcal{H}$ itself and $(X\mathcal{H})^{-1} = X^{-1}\mathcal{H}]$,

called the *quotient group* or *factor group* and denoted $\mathcal{G}/\mathcal{H}$.

The centre of $\mathcal{G}$ is an invariant subgroup of $\mathcal{G}$. Every subgroup of an Abelian group is invariant. Given a homomorphism from a group $\mathcal{G}$ onto some other group $\mathcal{G}'$, the set of elements mapped into the identity element of $\mathcal{G}'$ form an invariant subgroup $\mathcal{H}$ of $\mathcal{G}$ and $\mathcal{G}'$ is isomorphic to the factor group $\mathcal{G}/\mathcal{H}$.

Suppose $\mathcal{G}, \mathcal{H}$ are groups. The *direct product* group $\mathcal{G} \otimes \mathcal{H}$ is made up of ordered pairs of elements $(G, H), G \in \mathcal{G}, H \in \mathcal{H}$, with the multiplication defined by $(G_1, H_1)(G_2, H_2) = (G_1 G_2, H_1 H_2)$. It is of order $|\mathcal{G} \otimes \mathcal{H}| = |\mathcal{G}| \cdot |\mathcal{H}|$. The order of the element (G, H) is the least common multiple of the orders of G and H. (This implies that the direct product $\mathcal{C}_m \otimes \mathcal{C}_n$ of two cyclic groups is cyclic, namely $\mathcal{C}_{mn}$, if and only if m and n have no common factor.)

If a group $\mathcal{G}$ has two subgroups $\mathcal{H}_1, \mathcal{H}_2$ such that (i) $\mathcal{H}_1$ and $\mathcal{H}_2$ have no common element except the identity E, (ii) every element of $\mathcal{H}_1$ commutes with every element of $\mathcal{H}_2$ and (iii) $\mathcal{G} = \mathcal{H}_1 \mathcal{H}_2$, then $\mathcal{G}$ is isomorphic to the direct product $\mathcal{H}_1 \otimes \mathcal{H}_2$. It is common practice to say $\mathcal{G}$ *is* the direct product of $\mathcal{H}_1$ and $\mathcal{H}_2$. It can be shown that if $\mathcal{A}$ and $\mathcal{B}$ are subgroups of order a and b respectively, and if their intersection, which is a subgroup of both of them, has order d, then the complex $\mathcal{AB}$ has ab/d distinct elements and is a group if and only if $\mathcal{A}$ and $\mathcal{B}$ commute.

Examples

1. The cyclic group C_6 made up of $A^n, n = 1, \ldots, 6, A^6 = E$ has the (invariant) subgroups $\{E, A^3\}$ and $\{E, A^2, A^4\}$. These are isomorphic to C_2 and C_3, respectively. The cosets relative to C_2 are $\{E, A^3\}, \{A, A^4\}, \{A^2, A^5\}$ and the quotient group is isomorphic to C_3. The cosets relative to C_3 are $\{E, A^2, A^4\}, \{A, A^3, A^5\}$ and the quotient group is isomorphic to C_2. The group C_6 is a direct product $C_2 \otimes C_3$.

2. The group of symmetries of the equilateral triangle is of order 6, with elements $\{1, r_1, r_2, m_1, m_2, m_3\}$. The classes are $\{1\}, \{r_1, r_2\}, \{m_1, m_2, m_3\}$. The proper subgroups are $\{1, r_1, r_2\}, \{1, m_1\}, \{1, m_2\}, \{1, m_3\}$, of which only the first (made up entirely of complete classes) is invariant. Relative to the invariant subgroup, which is isomorphic to C_3, the cosets are $\{1, r_1, r_2\}, \{m_1, m_2, m_3\}$ and the quotient group is isomorphic to C_2. Relative to $\{1, m_1\}$, for instance, the left cosets are $\{1, m_1\}, \{r_1, m_3\}, \{r_2, m_2\}$ and the right cosets are $\{1, m_1\}, \{r_1, m_2\}$, and $\{r_2, m_3\}$, which are different. [Note that the direct product $\{1, r_1, r_2\} \otimes \{1, m_1\}$, for example, is not equal to the original group,

although all elements of the group can be formed from products of the elements of the subgroups. Since the elements of the two subgroups do not all commute, the multiplication table of the direct product group is different from that of the original group. The direct product group is isomorphic to C_6, as it must be, from example 1.]