The Commutator Subgroup

Math 430 - Spring 2013

Let G be any group. If $a, b \in G$, then the *commutator* of a and b is the element $aba^{-1}b^{-1}$. Of course, if a and b commute, then $aba^{-1}b^{-1} = e$. Now define C to be the set

$$C = \{x_1x_2\cdots x_n \mid n \geq 1, \text{ each } x_i \text{ is a commutator in } G\}.$$

In other words, C is the collection of all finite products of commutators in G. Then we have

Proposition 1. *If G is any group, then $C \lhd G$.*

Proof. First, we have $e = eee^{-1}e^{-1} \in C$, so C is nonempty and contains the identity. If $c, d \in C$, then we have $c = x_1x_2\cdots x_n$ and $d = y_1y_2\cdots y_m$, where each x_i and each y_j is a commutator in G. Then

$$cd = x_1x_2\cdots x_ny_1y_2\cdots y_m \in C,$$

since this is just another finite product of commutators. We also have

$$d^{-1} = (x_1x_2\cdots x_n)^{-1} = x_n^{-1}\cdots x_2^{-1}x_1^{-1}.$$

If $x_i = a_ib_ia_i^{-1}b_i^{-1}$, then $x_i^{-1} = b_ia_ib_i^{-1}a_i^{-1}$, which is also a commutator. Thus $c^{-1} \in C$, and $C \leq G$.

To prove C is a normal subgroup of G, let $g \in G$, and $c = x_1x_2\cdots x_n \in C$. Then we have

$$gcg^{-1} = gx_1x_2\cdots x_ng^{-1} = (gx_1g^{-1})(gx_2g^{-1})\cdots(gx_ng^{-1}), \tag{1}$$

where we have just inserted $gg^{-1} = e$ between x_i and x_{i+1} for each $i < n$. Now, if $x_i = a_ib_ia_i^{-1}b_i^{-1}$, then we have

$$gx_ig^{-1} = ga_ib_ia_i^{-1}b_i^{-1}g^{-1} = (ga_ig^{-1})(gb_ig^{-1})(ga_i^{-1}g^{-1})(gb_i^{-1}g^{-1}).$$

Now note that $(ga_ig^{-1})^{-1} = (g^{-1})^{-1}a_i^{-1}g^{-1} = ga_i^{-1}g^{-1}$, and we have the analogous statement if we replace a_i by b_i. So, we have

$$gx_ig^{-1} = (ga_ig^{-1})(gb_ig^{-1})(ga_ig^{-1})^{-1}(gb_ig^{-1})^{-1},$$

which is a commutator. Now, from (1), we have gcg^{-1} is a product of commutators, and so $gcg^{-1} \in C$. Thus $C \lhd G$. □

The subgroup C of G is called the *commutator subgroup* of G, and it general, it is also denoted by $C = G'$ or $C = [G, G]$, and is also called the *derived subgroup* of G. If G is Abelian, then we have $C = \{e\}$, so in one sense the commutator subgroup may be used as one measure of how far a group is from being Abelian. Specifically, we have the following result.

Theorem 1. *Let G be a group, and let C be its commutator subgroup. Suppose that $N \lhd G$. Then G/N is Abelian if and only if $C \subseteq N$. In particular, G/C is Abelian.*

Proof. First assume that G/N is Abelian. Let $a, b \in G$. Since we are assuming that G/N is Abelian, then we have $(aN)(bN) = (bN)(aN)$, and so $abN = baN$ by the definition of coset multiplication in the factor group. Now, we know $abN = baN$ implies $ab(ba)^{-1} \in N$, where $ab(ba)^{-1} = aba^{-1}b^{-1}$, and so $aba^{-1}b^{-1} \in N$. Since a and b were arbitrary, any commutator in G is an element of N, and since N is a subgroup of G, then any finite product of commutators in G is an element of N. Thus $C \subseteq N$.

Now suppose that $C \subseteq N$, and let $a, b \in G$. Then $aba^{-1}b^{-1} \in N$, and so $ab(ba)^{-1} \in N$. This implies $abN = baN$, or that $(aN)(bN) = (bN)(aN)$. Since a and b were arbitrary, this holds for any elements $aN, bN \in G/N$, and thus G/N is Abelian. □

Given a group G, and its derived subgroup G', we may then consider the derived subgroup of G', or $[G', G'] = (G')'$. This is often denoted as $G^{(2)}$. For any integer $i \geq 0$, define the i^{th} *derived subgroup* of G, denoted $G^{(i)}$, recursively as follows. Let $G^{(0)} = G$, and for $i \geq 1$, define $G^{(i)} = (G^{(i-1)})' = [G^{(i-1)}, G^{(i-1)}]$. By Theorem 1, note that we have $G^{(i)} \lhd G^{(i-1)}$, and by Theorem 1, $G^{(i-1)}/G^{(i)}$ is abelian, for all $i \geq 1$.

Recall that, from the first Homework, we may define a finite group G to be *solvable* if there are subgroups $H_0 = \{e\}, H_1, \ldots, H_k = G$, such that $H_0 \lhd H_1 \lhd \cdots \lhd H_k$, and H_i/H_{i-1} is abelian for each $i = 1, \ldots, k$. As we see now, the commutator subgroups are the key for understanding whether a finite group G is solvable.

Theorem 2. *Let G be a finite group. Then G is solvable if and only if there exists some integer $k \geq 0$ such that the k^{th} derived subgroup of G is trivial, that is, $G^{(k)} = \{e\}$.*

Proof. Let $k \geq 0$ such that $G^{(k)} = \{e\}$. By Proposition 1, we have $G^{(i)} \lhd G^{(i-1)}$ for any $i \geq 1$, so

$$\{e\} = G^{(k)} \lhd G^{(k-1)} \lhd \cdots \lhd G^{(2)} \lhd G^{(1)} = G' \lhd G^{(0)} = G.$$

Since $G^{(i-1)}/G^{(i)}$ is abelian for $i \geq 1$ by Theorem 1, then the existence of this subnormal series implies that G is solvable (taking $H_i = G^{(k-i)}$ in the definition).

Now assume that G is solvable. Then there are subgroup $\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_k = G$ such that H_i/H_{i-1} is abelian for $i = 1, \ldots, k$. In particular, $H_k/H_{k-1} = G/H_{k-1}$ is abelian, and so $G' \subset H_{k-1}$ by Theorem 1. By induction, suppose that $G^{(i)} \subset H_{k-i}$ for an $i \geq 1$. Since H_{k-i}/H_{k-i-1} is abelian, then $H'_{k-i} \subset H_{k-i-1}$ by Theorem 1. By the induction hypothesis, $G^{(i)} \subset H_{k-i}$, and so every commutator in $G^{(i)}$ is a commutator in H_{k-i}, which implies $(G^{(i)})' \subset H'_{k-i}$. Since $(G^{(i)})' = G^{(i+1)}$ and $H'_{k-i} \subset H_{k-i-1}$, we have $G^{(i+1)} \subset H_{k-i-1}$. By induction, we then have $G^{(k)} \subset H_0 = \{e\}$. Thus $G^{(k)} = \{e\}$. □

Theorem 2 is extremely useful for proving facts about finite solvable groups. For example, let G be any finite group, and suppose $H \leq G$. Then $H' \leq G'$ since every commutator of H is a commutator of G, and by induction $H^{(i)} \leq G^{(i)}$ for every $i \geq 0$. If G is solvable, then $G^{(k)} = \{e\}$ for some k. Since $H^{(k)} \leq G^{(k)}$, then $H^{(k)} = \{e\}$ and thus H is also solvable. This statement is true for an arbitrary group as well, but the argument is a bit more subtle.

Proposition 2. *Let G be any group, and suppose $H \leq G$. If G is solvable, then H is solvable.*

Proof. Recall that the definition of an arbitrary group being solvable (finite or not) in Fraleigh is that it has a decomposition series such that every decomposition factor group is abelian, and thus cyclic of prime order. So, suppose that

$$\{e\} = K_0 \lhd K_1 \lhd \cdots \lhd K_{m-1} \lhd K_m = G,$$

such that K_i/K_{i-1} is cyclic of prime order, for $i = 1, \ldots, m$. For each i, consider $H \cap K_i$. Recall the second isomorphism theorem of groups, which states that if L is a group, $N \lhd L$, and $M \leq N$, then $NM/N \cong M/(M \cap N)$. For $i = 1, \dots, m$, apply this theorem to the case that $L = K_i$, $N = K_{i-1}$, and $M = H \cap K_i$. Then we have

$$K_{i-1}(H \cap K_i)/K_{i-1} \cong (H \cap K_i)/(H \cap K_{i-1}),$$

since $M \cap N = H \cap K_i \cap K_{i-1} = H \cap K_{i-1}$. We also have

$$K_{i-1}(H \cap K_i)/K_{i-1} \leq K_i/K_{i-1},$$

and since K_i/K_{i-1} is cyclic of prime order, then we must have $K_{i-1}(H \cap K_i)/K_{i-1}$ is either trivial or cyclic of prime order. So the same must be true of $(H \cap K_i)/(H \cap K_{i-1})$. Therefore, we can build a decomposition series H with decomposition factors being cyclic of prime order, by using the subgroups $H \cap K_i$ (and not using those that are repeated). Thus H is solvable. □