Cosets, factor groups, direct products, homomorphisms, isomorphisms

Sergei Silvestrov

Spring term 2011, Lecture 11

Contents of the lecture

- Cosets and the theorem of Lagrange.
- Direct products and finitely generated abelian groups.
- Homomorphisms and automorphisms of groups.
- Normal subgroups, Factor groups, simple groups
Cosets

Perhaps the most fundamental fact about subgroups $H$ of a finite group $G$ is that their orders are constrained. Certainly, we have $|H| \leq |G|$, but it turns out that $|H|$ must be a divisor of $|G|$. To prove this, we introduce the notion of coset.

Let $H \leq G$. First, introduce the following relations on $G$:

\[
a \sim_L b \iff a^{-1}b \in H,
\]
\[
a \sim_R b \iff ab^{-1} \in H.
\]

**Theorem 1.** Both $\sim_L$ and $\sim_R$ are equivalence relations on $G$. The equivalence classes of $\sim_L$ are

\[
aH = \{ ah : h \in H \},
\]

while the equivalence classes of $\sim_R$ are

\[
Ha = \{ ha : h \in H \}.
\]

**Definition 1.** The subset $aH$ is called the **left coset** of $H$ containing $a$. The subset $Ha$ is called the **right coset** of $H$ containing $a$.

**Example 1.** Let $G = S_3$ and $H = \langle (1, 2) \rangle$. There are exactly three left cosets of $H$, namely

\[
H = \{ (1), (1, 2) \},
\]
\[
(1, 3)H = \{ (1, 3), (1, 2, 3) \},
\]
\[
(2, 3)H = \{ (2, 3), (1, 3, 2) \},
\]

each of which has size 2. The right cosets are

\[
H = \{ (1), (1, 2) \},
\]
\[
H(1, 3) = \{ (1, 3), (1, 3, 2) \},
\]
\[
H(2, 3) = \{ (2, 3), (1, 2, 3) \}.
\]

Again, we see that there are exactly 3 right cosets, each of which has size 2.
Lagrange’s Theorem

The next theorem is named after J. L. Lagrange, who saw, in 1770, that the order of certain subgroups of $S_n$ are divisors of $n!$.

**Theorem 2** (Lagrange’s Theorem). If $H$ is a subgroup of a finite group $G$, then $|H|$ is a divisor of $|G|$.

**Proof.** Let $\{a_1H, a_2H, \ldots, a_tH\}$ be the family of all the distinct cosets of $H$ in $G$. It follows that

$$|G| = |a_1H| + |a_2H| + \cdots + |a_tH|.$$ The mapping $h \mapsto ah$ is a one-to-one correspondence between $H$ and $aH$. It follows that $|a_jH| = |H|$ for all $j = 1, 2, \ldots, t$, so that $|G| = t|H|$, as desired. \qed

**Corollaries to Lagrange’s theorem**

**Corollary 1.** Every group of prime order is cyclic.

**Corollary 2.** The order of an element of a finite group divides the order of the group.

**Definition 2.** Let $H \leq G$. The **index of $H$ in $G$** is the number of left cosets of $H$ in $G$:

$$[G : H] = \frac{|G|}{|H|}.$$

**Corollary 3.** Let $K \leq H \leq G$ and suppose $(H : K)$ and $(G : H)$ are both finite. Then $(G : K)$ is finite and $(G : K) = (G : H)(H : K)$. 

The Cartesian products of finitely many structures

**Definition 3.** Let $S_1, S_2, \ldots, S_n$ be non-empty sets. The **Cartesian product of sets** $S_1, S_2, \ldots, S_n$ is the set

$$\{ (a_1, a_2, \ldots, a_n) : a_1 \in S_1, a_2 \in S_2, \ldots, a_n \in S_n \}.$$ 

It is denoted either by $S_1 \times S_2 \times \cdots \times S_n$ or by $\prod_{j=1}^n S_j$.

**Theorem 3.** Let $G_1, G_2, \ldots, G_n$ be groups. The Cartesian product $\prod_{j=1}^n G_j$ is a group under the binary operation

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n).$$

**Definition 4.** Under multiplicative notation, the group described in Theorem 10 is called the **direct product of the groups** $G_j$. Under additive notation, it is called the **direct sum of the groups** $G_j$. 

-- Typeset by FoilTEX --
Example: the direct products $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$

Example 2. Let $m$ and $n$ be relatively prime natural numbers, each greater than or equal to 2. Let $\phi: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ be the map $\phi(r) = (r \mod m, r \mod n)$. It is straightforward to show that this map is one-to-one correspondence and an isomorphism of groups.

If the greatest common divisor of $m$ and $n$ is $d > 1$, then, for any $(r, s) \in \mathbb{Z}_m \times \mathbb{Z}_n$, we have $(mn/d)(r, s) = (0, 0)$. It follows that $(r, s)$ does not generate the entire group $\mathbb{Z}_m \times \mathbb{Z}_n$. Therefore this group is not cyclic.

One can use this proof repeatedly. For example, $\mathbb{Z}_{30}$ is isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_6$, and $\mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_2$, so $\mathbb{Z}_{30}$ is isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_2$.

In general, let $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ be the prime decomposition of $n$. Then $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_k^{m_k}}$.

The least common multiple

Let $r_1$, $r_2$, $\ldots$, $r_k$ be positive integers. All integers divisible by each $r_j$ for $j = 1, 2, \ldots, k$ form the cyclic group.

Definition 5. The positive generator of the above mentioned cyclic group is called the least common multiple of the positive integers $r_1, r_2, \ldots, r_k$.

Theorem 4. A positive integer $n$ is the least common multiple of positive integers $r_1, r_2, \ldots, r_k$ if and only if $n$ is the smallest positive integer that is a multiple of each $r_j$ for $j = 1, 2, \ldots, k$.

Theorem 5. Let $(a_1, \ldots, a_n) \in \prod_{j=1}^n G_j$. If $a_j$ is of finite order $r_j$ in $G_j$, then the order of $(a_1, \ldots, a_n)$ in $\prod_{j=1}^n G_j$ is equal to the least common multiple of all the $r_j$. 
The Fundamental Theorem of finitely generated abelian groups

**Theorem 6.** Every finitely generated abelian group $G$ is isomorphic to a finite direct sum of cyclic groups, each of which is either infinite or of order a power of a prime. The direct sum is unique except for possible rearrangement of the factors.

In other words, $G$ is isomorphic to

$$
\mathbb{Z}_{p_1}^{m_1} \times \mathbb{Z}_{p_2}^{m_2} \times \cdots \times \mathbb{Z}_{p_k}^{m_k} \times \mathbb{Z}^r,
$$

where the $p_j$ are primes, the $m_j$ are positive integers, and $r$ is a nonnegative integer (the Betti number of $G$).
Example: all finite abelian groups of order 1500

Example 3. By Theorem 6, there exists a one-to-one correspondence between the set of all finite abelian groups of order 1500 and the representations

\[ 1500 = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}. \]  

(1)

Since the prime decomposition of 1500 is 1500 = 2^2 \cdot 3 \cdot 5^3, we proceed as follows. The number 2 that corresponds to 2^2, has two different partitions (representations as a sum of positive integers):

\[ 2 = 2, \]
\[ 2 = 1 + 1. \]

The number 1 that corresponds to 3 = 3^1, has only one partition 1 = 1. The number 3 that corresponds to 5^3, has three different partitions:

\[ 3 = 3, \]
\[ 3 = 1 + 2, \]
\[ 3 = 1 + 1 + 1. \]

By the Fundamental Counting Principle, there exists \(2 \cdot 1 \cdot 3 = 6\) different representations (1) that correspond to the following 6 possible abelian groups of order 1500.

<table>
<thead>
<tr>
<th>Representation</th>
<th>Abelian group</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2^2 \cdot 3 \cdot 5^3)</td>
<td>(\mathbb{Z}_4 \times \mathbb{Z}<em>3 \times \mathbb{Z}</em>{125})</td>
</tr>
<tr>
<td>(2^2 \cdot 3 \cdot 5 \cdot 5^2)</td>
<td>(\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}<em>5 \times \mathbb{Z}</em>{25})</td>
</tr>
<tr>
<td>(2^2 \cdot 3 \cdot 5 \cdot 5^3)</td>
<td>(\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5)</td>
</tr>
<tr>
<td>(2 \cdot 2^2 \cdot 3 \cdot 5^3)</td>
<td>(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}<em>3 \times \mathbb{Z}</em>{125})</td>
</tr>
<tr>
<td>(2 \cdot 2 \cdot 3 \cdot 5^2 \cdot 5^2)</td>
<td>(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}<em>5 \times \mathbb{Z}</em>{25})</td>
</tr>
<tr>
<td>(2 \cdot 2 \cdot 3 \cdot 5^5 \cdot 5^5)</td>
<td>(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5)</td>
</tr>
</tbody>
</table>
Homomorphisms of groups

Some motivating words and thoughts of wisdom!

By Cayley’s theorem any whatever small or big group $G$ can be found inside the symmetric group of all permutations on enough many elements and more specifically Cayley’s theorem states that can be always done inside $S_{|G|}$.

So, for example a group of 8 elements can be found inside the symmetric group $S_8$ consisting of $8! = 40320$ elements.

OBS! The sequence $n!$ grows enormously fast. The standard realization in the proof of Cayley’s theorem is important for investigation of groups and for applications where how large the size of the symmetric group is not so important (many such applications exists in physics, like solid state physics, nano-physics, those thermodynamics models where the behavior of the systems with $n \to \infty$ is studied, etc ...) However, for computational applications, such realization of the group inside another group of huge size can be of limited use already for modestly large $n$.

Thus important class of problem is to find a reasonably easy describable and computationally easy to use class of groups with as little as possible (or as "optimal" as possible) number of elements $n$, so that all groups from the subclass of groups specific for the application can be somehow realized inside this class.

There are many research problems of this type which are open and interesting for applications.

The above is just one important motivation and there are many more fundamental motivations for the importance of studying properties of mappings from a group to other groups $f: G \to H$ which "transfer/find" the multiplication and thus all or some of the properties of $G$ inside $H$:

$$f(g *_G h) = f(g) *_H f(h)$$

Such mappings are called homomorphisms of groups. Homomorphism with is moreover bijective (one-to-one) is called isomorphism.

Homomorphism of a group to the group of all invertible (under composition) linear operators on a linear space, or correspondingly, to the group of all invertible square matrices (under matrix multiplication) of some fixed size is called linear representation of the group (or sometimes matrix representation of the group in case matrices). The dimension of the linear space (the number of columns/rows in the representing matrices) is called then the dimension of the representation.
The area studying linear representations of groups is called Theory of group representations.

The theory of representations play very important and often absolutely crucial and fundamental role in many parts of physics, engineering, chemistry, biology, and more ......

Many Nobel prizes, Fields medals, and technological and scientific breakthroughs came alive as a result of the study or clever use of linear representations of groups (of rings and of other algebraic structures).

Another related important problem is determining whether two given groups $G$ and $H$ are somehow the same (equivalent or isomorphic) 

More general problem is that of classification of all groups with respect to isomorphism. In general this problem is widely open. It is solved only for some classes of groups, for example for finite abelian groups and for so called finite simple groups. These and other classifications play very important role in nuclear, solid state, nano and other parts of physics, in chemistry, in coding algorithms, in investigation of symmetries and in many other cases.
Homomorphisms of groups (cont.)

**Definition 6.** If \((G, \ast)\) and \((H, \circ)\) are groups, then a function \(\varphi : G \rightarrow H\) is a **homomorphism** if

\[
\varphi(x \ast y) = \varphi(x) \circ \varphi(y)
\]

for all \(x, y \in G\).

The word *homomorphism* comes from the Greek *homo* meaning “same” and *morph* meaning “shape” or “form”. Thus, a homomorphism carries a group to another group (its image) of similar form.

Examples of homomorphisms

**Example 4.** Let \(G\) be an abelian group. The map \(x \mapsto x^{-1}\) of \(G\) into itself is a homomorphism. In additive notation, this map looks like \(x \mapsto -x\). The verification that it has the property defining a homomorphism is immediate.

**Example 5.** The map \(z \mapsto |z|\) is a homomorphism of the group \(\mathbb{C}^*\) into \(\mathbb{R}^+\).

**Example 6.** The map \(x \mapsto e^x\) is a homomorphism of the group \((\mathbb{R}, +)\) into the group \((\mathbb{R}^+, \cdot)\). Its inverse map, the logarithm, is also a homomorphism.

**Example 7.** Recall that a linear transformation \(T : \mathbb{R}^n \rightarrow \mathbb{R}^n\) has the property that \(T(a + b) = T(a) + T(b)\). Thus \(T\) is a group homomorphism from the additive group \(\mathbb{R}^n\) to itself. More concretely, for any \(n\)-by-\(n\) matrix \(M\), we have \(M(a + b) = Ma + Mb\). Thus multiplication by \(M\) is a group homomorphism from the additive group \(\mathbb{R}^n\) to itself.
Properties, kernels and images of homomorphisms

**Definition 7.** If \( \varphi : G \rightarrow H \) is a homomorphism, define the kernel of \( \varphi \) as
\[
\ker(\varphi) = \varphi^{-1}(e),
\]
and the image of \( \varphi \) as
\[
\text{Im}(\varphi) = \varphi[G].
\]

*Kernel comes from the German word meaning “grain” or “seed” (corn comes from the same word).*

**Example 8.** A map that maps any even permutation in \( S_n \) to 1 and any odd permutation to \(-1\) is homomorphism of \( S_n \) to the multiplicative group \( \{\pm 1\} \). Its kernel is the alternating group \( A_n \).

**Example 9.** Determinant is an onto homomorphism of the group \( \text{GL}(n, \mathbb{R}) \) of invertible \( n \times n \) matrices to the multiplicative group of nonzero real numbers \( \mathbb{R}^\times \), whose kernel is the special linear group \( \text{SL}(n, \mathbb{R}) \) of all \( n \times n \) matrices of determinant 1.

**Theorem 7.** Theorem 7.19 expanded

Let \( \varphi : G \rightarrow H \) be a homomorphism of groups.

- \( \varphi(1_G) = 1_{G'} \).
- \( \varphi(x^{-1}) = \varphi(x)^{-1} \).
- \( \varphi(x^n) = \varphi(x)^n \) for all \( n \in \mathbb{Z} \).
- \( \exists \varphi = \varphi(G) \) is a subgroup of \( H \).
- \( \ker(\varphi) := \{ g \in G | \varphi(g) = 1_{G'} \} = \varphi^{-1}(\{1_{G'}\}) \) is a subgroup of \( G \).

**Proof.**

1. \( 1_G \cdot 1_G = 1_G \) implies \( \varphi(1_G)\varphi(1_G) = \varphi(1_G) \).
2. \( 1 = xx^{-1} \) implies \( 1_{G'} = \varphi(1_G) = \varphi(x)\varphi(x)^{-1} \).
3. Use induction to show that \( \varphi(x^n) = \varphi(x)^n \) for all \( n \geq 0 \). Then observe that \( x^{-n} = (x^{-1})^n \), and use part 2.
4. \( \exists \varphi \) is a subgroup of \( G' \) since it contains \( 1_{G'} \) by part 1, is closed under the operation of taking inverse in \( G' \) by part 2, and is closed under operation of multiplication in \( G' \) by homomorphism property \( \varphi(x *_{G'} y) = \varphi(x) *_{G'} \varphi(y) \).
5. \( \ker \varphi \) is a subgroup of \( G \) since it contains \( 1_G \) by part 1, is closed under the operation of taking inverse in \( G \) by part 2 because
\[
\varphi(x^{-1}) = \varphi(x)^{-1} = 1_{G'}^{-1} = 1_{G'} \text{ for } x \in \ker \varphi
\]
and Ker $\varphi$ is closed under operation of multiplication in $G$ by homomorphism property

$$\varphi(x \ast_G y) = \varphi(x) \ast_{G'} \varphi(y) = 1_{G'} 1_{G'} = 1_{G'}$$
An important property of a kernel. Normal subgroups.

**Theorem 8.** Let $\varphi : G \rightarrow G'$ be a homomorphism of groups with kernel $H = \text{Ker} \, \varphi$. Let $a \in G'$, and let $X = \varphi^{-1}(a)$. Then, for any $u \in X$, $X = uH = Hu$.

Since clearly any $u \in G$ is in $\varphi^{-1}(a)$ for some $a \in G'$, the property $uH = Hu$ holds for any $u$.

In other words, the partitions of $G$ into left cosets and into right cosets of $H$ is the same.

**Proof.** Let $u \in X$ so by definition of $X$, $\varphi(u) = a$. We first prove $uH \subseteq X$. For any $h \in H$,

$$\varphi(uh) = \varphi(u)\varphi(h)$$

since $\varphi$ is a homomorphism

$$= \varphi(u)1$$

since $h \in \text{ker}(\varphi)$

$$= a,$$

that is, $uh \in X$. This proves $uH \subseteq X$. To establish the reverse inclusion suppose $g \in X$ and let $h = u^{-1}g$. Then

$$\varphi(h) = \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}\varphi(g) = a^{-1}a = 1.$$ 

Thus $h \in \text{Ker}(\varphi)$. Since $h = u^{-1}g$, $g = uh \in uH$, establishing the inclusion $X \subseteq uH$. The equality $X = Hu$ is proved, using the same patterns.

Normal subgroups

**Definition 8.** A subgroup $H$ of a group $G$ is **normal** if the partitions of $G$ into left cosets and into right cosets of $H$ is the same.

**Theorem 8** says that the kernel of a group homomorphism is a normal subgroup. Later we will see that the inverse statement is also true.

**Theorem 9.** *(Theorem 7.51)* The alternating group $A_n$ is a normal subgroup in $S_n$ (and $|A_n| = \frac{n!}{2}$)

**Proof.** By the previous general theorems kernel of any homomorphism is a normal subgroup. Therefore, $A_n$ is a normal subgroup of $S_n$ because it is the kernel of the "parity" homomorphism $\varphi : S_n \rightarrow \mathbb{Z}_2$ defined by

$$\varphi(\sigma) = \begin{cases} 
\varphi(\sigma) = 0 & \text{if } \sigma \text{ is even} \\
\varphi(\sigma) = 1 & \text{if } \sigma \text{ is odd}
\end{cases}$$
OBS! Exercise! Can you prove that this is a homomorphism?
Factor groups from homomorphisms

**Theorem 10.** Let $\varphi : G \rightarrow G'$ be a group homomorphism with $H = \text{Ker}(\varphi)$. Then the coset multiplication
\[(aH)(bH) = (ab)H\]
is well defined, independent of the choices $a$ and $b$ from the cosets, and makes the set $G/H$ of left cosets into a group (factor group). The map $\mu : G/H \rightarrow \varphi[G]$ defined by
\[\mu(aH) = \varphi(a)\]
is an isomorphism, independent of the choice of $a$ from the coset.

**Example: the residue classes**

**Example 10.** Let $G = \mathbb{Z}$, let $G' = \mathbb{Z}_n$ and let $\gamma : \mathbb{Z} \rightarrow \mathbb{Z}_n$ maps an integer $m \in \mathbb{Z}$ to the reminder $\gamma(m)$ when $m$ is divided by $n$. Let
\[m = q_1n + r_1 \quad \text{and} \quad p = q_2n + r_2,\]
where $0 \leq r_i < n$ for $i = 1, 2$. It means that $\gamma(m) = r_1$ and $\gamma(p) = r_2$. If $r_1 + r_2 = q_3n + r_3$ for $0 \leq r_3 < n$, then $r_1 + r_2 = r_3$. Adding the two display equations gives
\[m + p = (q_1 + q_2 + q_3)n + r_3,\]
so that $\gamma(m + p) = r_3 = r_1 + r_2$. So $\gamma$ is a homomorphism.

The kernel of $\gamma$ is $n\mathbb{Z}$. By Theorem 10, the factor group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. The cosets of $n\mathbb{Z}$ are the residue classes modulo $n$. The isomorphism $\gamma : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}_n$ assigns to each residue class its smallest nonnegative element.
Factor groups from normal subgroups

**Theorem 11.** Let $H$ be a subgroup of a group $G$. The coset multiplication

$$(aH)(bH) = (ab)H$$

is well defined, independent of the choices $a$ and $b$ from the cosets, and makes the set $G/H$ of left cosets into a group if and only if $H$ is a normal subgroup of $G$.

The fundamental homomorphism theorem

**Theorem 12.** If $\varphi: G \rightarrow G'$ is a homomorphism with kernel $H$, then $\varphi[G]$ is a group, and $\mu: G/H \rightarrow \text{Im}(\varphi) \leq G'$ given by $\mu(gH) = \varphi(g)$ is an isomorphism. If $\gamma: G \rightarrow G/H$ is the homomorphism given by $\gamma(g) = gH$, then $\varphi = \mu \circ \gamma$. 

\[G \xrightarrow{\gamma} G/H \xrightarrow{\mu} \varphi[G] \leq G'\]
Inner automorphisms

**Definition 9.** A isomorphism $\varphi : G \to G$ of a group $G$ with itself is an automorphism of $G$. The automorphism $i_g : G \to G$ defined by

$$i_g(x) = gxg^{-1}, \quad x \in G,$$

is the inner automorphism of $G$ by $g$. Performing $i_g$ on $x$ is called conjugation of $x$ by $g$.

**Theorem 13.** If $H$ is a subgroup of a group $G$, then the following conditions are equivalent

1. the partitions of $G$ into left cosets and into right cosets of $H$ is the same;
2. $gH = Hg$ for all $g \in G$;
3. $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$;
4. $gHg^{-1} = H$ for all $g \in G$. 
Simple groups

Definition 10. A group $G$ is simple if $G \neq \{e\}$ and has no proper nontrivial normal subgroups.

Theorem 14. (Theorem 7.52) If $n \geq 5$, then the alternating group $A_n$ is simple.

The classification of finite simple groups was completed in 1980. Efforts by several hundreds mathematicians covering around 500 papers between 5000 and 10000 journal pages have resulted in the proof of the following theorem.

Theorem 15. There is a list containing 18 infinite families of simple groups and 26 simple groups not belonging to these families (the sporadic simple groups) such that every finite simple group is isomorphic to one of the groups in this list.

Let $N$ be a normal subgroup of $G$. We would like to find when the factor group $G/N$ is a simple group.

Theorem 16. The factor group $G/M$ is simple if and only if $M$ is a maximal normal subgroup of $G$, i.e., $M \neq G$ and there is no proper normal subgroup $N$ of $G$ properly containing $M$. 

The centre and commutator subgroups

**Theorem 17.** If $G$ is a group, then $Z = \{ g \in G : gh = hg \text{ for all } g \in G \}$ is an abelian subgroup of $G$ (the centre) of $G$.

**Definition 11.** The **commutator subgroup** of a group $G$ is

$$C = \langle aba^{-1}b^{-1} : a, b \in G \rangle.$$

In other words, the commutator subgroup is the subgroup generated by **commutators** $aba^{-1}b^{-1}$.

**Theorem 18.** $C$ is a normal subgroup of $G$. For any normal subgroup $N$ of $G$, the factor group $G/N$ is abelian if and only if $C \leq N$. 