Cosets and direct products

Abdennour Kitouni, Anatoliy Malyarenko and Sergei Silvestrov

November 19, 2015

Abstract

Contents of the lecture.

- ☞ Cosets and the theorem of Lagrange.
- ☞ Direct products and finitely generated abelian 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:

$$a \sim_L b \Leftrightarrow a^{-1}b \in H,$$

$$a \sim_R b \Leftrightarrow ab^{-1} \in H.$$

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

$$aH = \{ah \colon h \in H\},$$

while the equivalence classes of $\sim_R$ are

$$Ha = \{ha \colon h \in H\}.$$

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. □

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

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

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*

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

Definition 4. Under multiplicative notation, the group described in Theorem 3 is called the **direct product of the groups** G_j. Under additive notation, it is called the **direct sum of the groups** G_j.

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 $\phi \colon \mathbb{Z}_{mn} \mapsto \mathbb{Z}_m \times \mathbb{Z}_n$ be the map $\phi(r) = (r \bmod m, r \bmod n)$. 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 $n = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$ 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

$$1500 = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}. \tag{1}$$

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.

Representation	Abelian group
$2^2 \cdot 3 \cdot 5^3$	$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_{125}$
$2^2 \cdot 3 \cdot 5 \cdot 5^2$	$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{25}$
$2^2 \cdot 3 \cdot 5 \cdot 5 \cdot 5$	$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$2 \cdot 2 \cdot 3 \cdot 5^3$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{125}$
$2 \cdot 2 \cdot 3 \cdot 5 \cdot 5^2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{25}$
$2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 5$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$