Study Material

Subject: Mathematics

Semester: 2nd

Name of Teacher: Prabir Rudra

Topic: Cosets, Lagrange's Theorem and Fermat's Little Theorem (CC-4)

Advice from faculty

The students of 2nd semester (Mathematics honours) are advised to read the enclosed study material on **Cosets, Lagrange's theorem and Fermat's Little theorem. We will arrange a doubt clearing session on this topic via video conferencing very soon. So the students are advised to read this material before attending the online session.** We will inform you about the date and time of the doubt clearing session.

In case of any difficulty regarding the topic the students may contact the concerned teacher via various media (e-mail, WhatsApp, Google classroom, etc.) and get their queries settled.

e-mail: prudra.math@gmail.com

Date: 09.05.2020

5.3 Cosets and Lagrange's Theorem

It is amazing to know that Lagrange's theorem, a distinct milestone in abstract algebra, a result which is of paramount importance in the theory of finite groups, was proved as early as in 1770, much before the formal inception of the concept of a group! Indeed, this was a period when eminent mathematicians all over Europe were busy trying to find a possible general *formula* (aptly known as solution by *radicals*) for the roots of a general polynomial equation (of degree n, say), explicitly in terms of its coefficients. After Sridharacharya's ancient solution for quadratic in 750 AD, the stage was set by H. Cardano (1501-1576) with such a solution for a cubic equation and then by L. Ferrari (1526-1565), one of his students, who successfully did it for a biquadratic. How nice it would be to have a general *formula*[4] for the roots of an nth degree polynomial, which might perhaps reduce to these particular cases on putting the respective values of $n = 2, 3, 4$ etc.! In this atmosphere, J.L. Lagrange (1736-1813) investigated the effects of permutations of the roots of a polynomial equation. Though he did not know it, his works[5] (1770) paved the path towards the concept of *permutation groups* in mathematics, the path that was appreciated only after almost 60 years by the genius of Galois, who in 1829 defined a finite group as a group of permutations. In this section, we shall discuss Lagrange's theorem and relevant results.

Definition 5.3.1. Let H be a subgroup of a group G. If $a \in G$, the subset $aH = \{ah \,|\, h \in H\}$ is called a ***left coset*** of H in G. Similarly, $Ha = \{ha \,|\, h \in H\}$ is called a ***right coset*** of H in G.

Observe that $eH = H = He$. Hence H is a left and right coset of itself in G.

Example 5.3.2. Let $G = \{1, a, b, ab\}$ be the Klein's four-group. Then $o(a) = o(b) = 2$, $ab = ba$. In this group, $H = \{1, a\}$ is a subgroup and $1H = \{1, a\}, aH = \{a, a^2\} = \{a, 1\} = \{1, a\}$, $bH = \{b, ba\} = \{b, ab\}$, $abH = \{ab, aba\} = \{ab, a^2b\} = \{ab, b\}$ are the left cosets of H in G.

[4]However, a result to the effect that such a dream is not to be fulfilled for equations of degree 5 is credited to Neils Heinrich Abel(1802-1829) of Norway. The corresponding general theory for equations of a higher degree is due to Galois.

[5]The famous Lagrange's theorem, in his contemporary terminology was as follows: *the number of distinct polynomials obtained from a polynomial in n variables by applying all possible permutations of the variables is a factor of n!* In modern day terminology of group theory it says : *the order of a subgroup of a finite group divides the order of that group*, which was actually formulated by Jordan in 1870.

Example 5.3.3. Consider the group $(\mathbb{Z}, +)$. Let $H = 5\mathbb{Z} = \{5n \mid n \in \mathbb{Z}\}$. H is a subgroup of the group $(\mathbb{Z}, +)$. Now the left cosets of H in $\mathbb{Z}$ are given by $n + H$ for all $n \in \mathbb{Z}$, i.e., $n + 5\mathbb{Z}$ for $n = 0, \pm 1, \pm 2, \ldots$

Any integer n is of the form $5m + r$, where $r = 0, 1, 2, 3$ or 4. Hence $n + 5\mathbb{Z} = 5m + r + 5\mathbb{Z} = r + 5m + 5\mathbb{Z} = r + 5\mathbb{Z}$. Hence the left cosets of $H = 5\mathbb{Z}$ in $\mathbb{Z}$ are $0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}$.

Example 5.3.4. Consider the symmetric group $S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$. In this group, $H = \{e, (1\,2)\}$ is a subgroup. The left cosets of H in S_3 are

$$\begin{aligned} eH &= H \\ (1\,2)H &= \{(1\,2), (1\,2)(1\,2)\} = \{(1\,2), e\} \\ (2\,3)H &= \{(2\,3), (2\,3)(1\,2)\} = \{(2\,3), (1\,3\,2)\} \\ (1\,3)H &= \{(1\,3), (1\,3)(1\,2)\} = \{(1\,3), (1\,2\,3)\} \\ (1\,2\,3)H &= \{(1\,2\,3), (1\,2\,3)(1\,2)\} = \{(1\,2\,3), (1\,3)\} \\ (1\,3\,2)H &= \{(1\,3\,2), (1\,3\,2)(1\,2)\} = \{(1\,3\,2), (2\,3)\}. \end{aligned}$$

Notice that any two left cosets of H in S_3 are either disjoint, e.g., $(2\,3)H$ and $(1\,3)H$ or, two left cosets are equal, e.g., $(2\,3)H$ and $(1\,3\,2)H$. Now all the distinct left cosets of H in S_3 are as follows:

$$H = \{e, (1\,2)\};\ (2\,3)H = \{(2\,3), (1\,3\,2)\};\ (1\,3)H = \{(1\,3), (1\,2\,3)\}.$$

Notice that $S_3 = H \cup (2\,3)H \cup (1\,3)H$ and $|H| = |(2\,3)H| = |(1\,3)H|$.

Next we compute all the right cosets of H in S_3. The right cosets of H in S_3 are Ha for all $a \in S_3$.

$$\begin{aligned} He &= H \\ H(1\,2) &= \{(1\,2), (1\,2)(1\,2)\} = \{(1\,2), e\} \\ H(2\,3) &= \{(2\,3), (1\,2)(2\,3)\} = \{(2\,3), (1\,2\,3)\} \\ H(1\,3) &= \{(1\,3), (1\,2)(1\,3)\} = \{(1\,3), (1\,3\,2)\} \\ H(1\,2\,3) &= \{(1\,2\,3), (1\,2)(1\,2\,3)\} = \{(1\,2\,3), (2\,3)\} \\ H(1\,3\,2) &= \{(1\,3\,2), (1\,2)(1\,3\,2)\} = \{(1\,3\,2), (1\,3)\}. \end{aligned}$$

For right cosets also, we find that, any two right cosets are either equal or disjoint. All the distinct right cosets of H in S_3 are as follows:

$$H = \{e, (1\,2)\};\ H(1\,3) = \{(1\,3), (1\,3\,2)\};\ H(2\,3) = \{(2\,3), (1\,2\,3)\}.$$

Here also $S_3 = H \cup H(1\,3) \cup H(2\,3)$ and $|H| = |H(1\,3)| = |H(2\,3)|$. But we note that a left coset aH may not be equal to the corresponding right coset Ha, e.g., $(2\,3)H \neq H(2\,3)$.

In the above example we see that all left cosets and right cosets of H in S_3 have the same number of elements, viz., 2. Also there are the same number of distinct left cosets of H in S_3, as of distinct right cosets, viz., 3. We now prove in the following theorem that these results hold in general for left and right cosets in any group.

Theorem 5.3.5. *Let H be a subgroup of a group G and let $a, b \in G$.*

(i) $aH = H$ *if and only if* $a \in H$.

(ii) $Ha = H$ *if and only if* $a \in H$.

(iii) $aH = bH$ *if and only if* $a^{-1}b \in H$.

(iv) $Ha = Hb$ *if and only if* $ba^{-1} \in H$.

(v) *Either* $aH \cap bH = \emptyset$ *or* $aH = bH$.

(vi) *Either* $Ha \cap Hb = \emptyset$ *or* $aH = Hb$.

Proof. (i) Suppose $aH = H$. Then $a = ae \in aH = H$. Conversely, suppose $a \in H$. Then for any $h \in H$, $h = eh = aa^{-1}h \in aH$ implies that $H \subseteq aH$. Since H is a subgroup and $a \in H$, we find that $aH = \{ah \mid h \in H\} \subseteq H$. Hence $H = aH$.

(ii) Proof is similar to (i).

(iii) Suppose $aH = bH$. Since $b = be \in bH = aH$, there exists $h \in H$ such that $b = ah$ for some $h \in H$. Then $a^{-1}b = h \in H$. Conversely, suppose $a^{-1}b \in H$. Hence $bH = aa^{-1}bH = a(a^{-1}bH) = aH$, since by (i), $a^{-1}b \in H$ implies $a^{-1}bH = H$.

(iv) Proof is similar to (iii).

(v) If $aH \cap bH \neq \emptyset$, there exists $x \in aH \cap bH$. Let $x = ah_1 = bh_2$ where $h_1, h_2 \in H$. Then $a^{-1}b = h_1h_2^{-1} \in H$, so $aH = bH$ by (iii).

(vi) Proof is similar to (v). □

Corollary 5.3.6. *Let H be a subgroup of a group G. Then $\{aH \mid a \in G\}$ forms a partition of G.*

Proof. Let $\mathcal{P} = \{aH \mid a \in G\}$, i.e., $\mathcal{P}$ is the set of all left cosets of H in G. By Theorem 5.3.5, for all $aH, bH \in \mathcal{P}$, either $aH \cap bH = \emptyset$ or $aH = bH$. Now for all $a \in G, aH \subseteq G$ and so $\bigcup_{a \in G} aH \subseteq G$. Again, if $a \in G$, then $a \in aH$ and hence $G \subseteq \bigcup_{a \in G} aH$. So we find that $G = \bigcup_{a \in G} aH$. Consequently, $\mathcal{P}$ is a partition of G. □

Theorem 5.3.7. *Let H be a subgroup of a group G. If $a \in G$, then $|aH| = |H| = |Ha|$.*

Proof. To show that $|H| = |aH|$, we show that there exists a bijective mapping of H onto aH. Define $f : H \to aH$ by $f(h) = ah$ for all $h \in H$. Let $h, h_1 \in H$. Suppose $f(h) = f(h_1)$. Then $ah = ah_1$ which implies that $h = h_1$ (by cancellation property) and so f is one-one. To show f is onto, let $ah \in aH$. Then $ah = f(h)$ and hence f maps H onto aH. Similarly, we can show that there exists a bijective mapping of H onto Ha. □

Theorem 5.3.8. *Let H be a subgroup of a group G. Then $|\mathcal{L}| = |\mathcal{R}|$, where $\mathcal{L}$ (resp.$\mathcal{R}$) denotes the set of all left (resp. right) cosets of H in G.*

Proof. To establish this, we need to show the existence of a bijective function from $\mathcal{L}$ onto $\mathcal{R}$. Define $f : \mathcal{L} \to \mathcal{R}$ by $f(aH) = Ha^{-1}$ for all $aH \in \mathcal{L}$. Observe that Ha^{-1} is a right coset of H in G and hence $Ha^{-1} \in \mathcal{R}$. Now, we show that $aH = bH$ if and only if $Ha^{-1} = Hb^{-1}$. Suppose $aH = bH$. Then $a^{-1}b \in H$. Hence $b^{-1}(a^{-1})^{-1} \in H$ and so by Theorem 5.3.5(iv), we have $Ha^{-1} = Hb^{-1}$.

Conversely, assume that $Ha^{-1} = Hb^{-1}$. Then by Theorem 5.3.5(iv), $b^{-1}(a^{-1})^{-1} \in H$, i.e., $b^{-1}a \in H$ and so $a^{-1}b = (b^{-1}a)^{-1} \in H$. Then by Theorem 5.3.5(iii), $aH = bH$. Thus we find that f is well-defined and one-one. Since for all $Ha \in \mathcal{R}$, $Ha = H(a^{-1})^{-1} = f(a^{-1}H)$ and $a^{-1}H \in \mathcal{L}$, f is onto. Thus f is a one-one and onto mapping. □

Definition 5.3.9. Let H be a subgroup of a group G. Then the number of distinct left (or right) cosets of H in G, written $[G : H]$, is called the ***index*** of H in G.

By Theorem 5.3.8, the number of distinct left cosets and the number of distinct right cosets of a subgroup H of a group G are the same. Thus, $[G : H]$ is well-defined.

Theorem 5.3.10. (Lagrange) *Let H be a subgroup of a finite group. Then the order of H divides the order of G. In particular,*

$$|G| = [G : H]|H|.$$

Proof. Since G is a finite group, $[G : H]$ is finite. Let $[G : H] = r$. This implies that there exist r distinct left cosets $a_1H, a_2H, \ldots, a_rH$ of H in G. Since distinct left cosets are mutually disjoint, we have

$$|G| = \left|\bigcup_{i=1}^{r} a_iH\right| = |a_1H| + |a_2H| + \ldots + |a_rH|$$

$$= \underbrace{|H| + |H| + \ldots + |H|}_{r \text{ times}} \quad \text{(by Theorem 5.3.7, } |a_i H| = |H|\text{)}$$

$$= r|H| = [G : H]\,|H|.$$

Hence the theorem. □

Note that by virtue of Lagrange's theorem, we have a useful formula to calculate the index of a subgroup H in a finite group G. Indeed,

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

Lagrange's theorem is a very useful theorem in finite groups. In the study of finite groups, we need this theorem most of the times. Let us now show some applications of this theorem.

Corollary 5.3.11. *Every group of prime order is cyclic.*

Proof. Let G be a group of prime order, say p. Since $p > 1$, G has an element $a \neq e$. Let H be the subgroup $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. By Lagrange's theorem, $|\langle a \rangle|$ divides p. Hence $|\langle a \rangle| = 1$ or p. Since $a \neq e$, $|\langle a \rangle| \neq 1$ and so $|\langle a \rangle| = p$. Now $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = |G| = p$. Hence, $G = \langle a \rangle$. This shows that G is a cyclic group. □

Since every cyclic group is commutative, the above corollary also tells us that *every group of prime order is commutative.*

Corollary 5.3.12. *Let G be a group of finite order n and $a \in G$. Then $o(a)$ divides n and $a^n = e$.*

Proof. Let $H = \langle a \rangle$. Then H is a cyclic subgroup of G and $|H| = o(a)$. By Lagrange's theorem, $|H|$ divides $|G|$. Hence $o(a)$ divides n. Let $o(a) = m$. Then $n = mk$ for some integer k. Now $a^m = e$ and hence $a^n = a^{mk} = (a^m)^k = e$. □

Our next result, known as *Fermat's little theorem*, is a result from number theory, which has been proved to be a powerful tool in *Cryptography*, the modern science of encoding and decoding messages. We show that this result can be proved by Largange's theorem.

Theorem 5.3.13. (Fermat) *Let p be a prime integer and a be an integer such that p does not divide a. Then $a^{p-1} \equiv 1 (mod p)$.*

Proof. For the prime integer p, $U_p = \{[a] \in \mathbb{Z}_p \mid gcd(a,p) = 1\}$. Then $U_p = \mathbb{Z}_p \backslash \{[0]\}$ is a group of order $p-1$. Let a be an integer such that p does not divide a. Then $[a]$ is a nonzero element of $\mathbb{Z}_p$ and so $[a] \in U_p$. Thus by Corollary 5.3.12, $[a]^{p-1} = [1]$, i.e., $[a^{p-1}] = [1]$. Hence $a^{p-1} \equiv 1 (\bmod p)$. □

Let H and K be two subgroups of a group G. If H and K are both finite, then $|HK|$ is finite but HK need not be a subgroup of G and so $|HK|$ need not divide $|G|$. However, with the help of Lagrange's theorem we can determine $|HK|$. This is a very useful result and we will use it very effectively in the sequel. In the next theorem, we determine $|HK|$ when H and K are both finite.

Theorem 5.3.14. *Let H and K be finite subgroups of a group G. Then*

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Proof. Let $A = H \cap K$. Since H and K are subgroups of G, A is a subgroup of G and so A is also a subgroup of H. By Lagrange's theorem, $|A|$ divides $|H|$. Let $n = \frac{|H|}{|A|}$. Then $[H : A] = n$ and so A has n distinct left cosets in H. Let $\{x_1A, x_2A, \ldots, x_nA\}$ be the set of all distinct left cosets of A in H. Then $H = \bigcup_{i=1}^{n} x_iA$. Since $A \subseteq K$, it follows that

$$HK = \Big(\bigcup_{i=1}^{n} x_iA\Big)K = \bigcup_{i=1}^{n} x_iK.$$

We now show that $x_iK \cap x_jK = \emptyset$ if $i \neq j$. Suppose $x_iK \cap x_jK \neq \emptyset$ for some $i \neq j$. Then $x_iK = x_jK$. Thus, $x_i^{-1}x_j \in K$. Since $x_i^{-1}x_j \in H$, we have $x_i^{-1}x_j \in A$ and so $x_iA = x_jA$. This contradicts the assumption that $x_1A, \ldots, x_nA$ are all distinct left cosets. Hence $x_1K, \ldots, x_nK$ are distinct left cosets of K. Also, $|K| = |x_iK|$ by Theorem 5.3.7, for all $i = 1, 2, \ldots, n$. Hence,

$$|HK| = |x_1K| + \ldots + |x_nK| = n|K| = \frac{|H||K|}{|A|} = \frac{|H||K|}{|H \cap K|}.$$

□

We conclude this section by showing that the converse of Lagrange's theorem is *not true in general.* We have shown in a finite cyclic group of order n that, for each divisor d of n, there exists a subgroup of order d. Hence the converse of Lagrange's theorem holds in a finite cyclic group. Now, we show that there are groups in which the converse of Lagrange's theorem does not hold.

Consider the symmetric group S_4. In this group, the set A_4 of all even permutations is a subgroup of order 12. Let us show that A_4 has no subgroup of order 6. Suppose, on the contrary that A_4 has a subgroup H of order 6. Now $(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (2\,3\,4), (2\,4\,3), (1\,3\,4)$, and $(1\,4\,3)$ are all even permutations and hence these are all members of A_4. Since $|H|$ is 6, H cannot contain all these 3-cycles. Let $\alpha = (a\,b\,c)$ be a 3-cycle such that $\alpha \notin H$. Now $o(\alpha) = 3$. Hence, $K = \{e, \alpha, \alpha^2\}$ is a subgroup of A_4. Note that $\alpha^2 = \alpha^{-1}$. Hence $H \cap K = \{e\}$. Then,

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = \frac{6 \cdot 3}{1} = 18.$$

But as $HK \subseteq A_4$, this contradicts the fact that $|A_4| = 12$. Consequently, A_4 has no subgroup of order 6. So we find that the converse of Lagrange's theorem does not hold in A_4.