PMATH 336: INTRODUCTION TO GROUP THEORY WITH APPLICATIONS
NOTES FOR WEEK 6

INSTRUCTOR: ARUNDHATHI KRISHNAN

7. Cosets and Lagrange's Theorem

7.1. Cosets.

Definition 7.1.1. Let G be a group and H be a non-empty subset of G. For any $a \in G$, the set $\{ah \mid h \in H\}$ is denoted by aH. Similarly, Ha denotes the set $\{ha \mid h \in H\}$ and aHa^{-1} the set $\{aha^{-1} \mid h \in H\}$. If H is a subgroup of G, aH is called the left coset of H in G containing a, and Ha is called the right coset of H in G containing a.

Example 7.1.2.

(i) Let $G = S_3, H = \{(1), (1,3)\}$. The left cosets of H in S_3 are:

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

(ii) Let $G = \mathbb{Z}_9$ and $H = \{0, 3, 6\}$. The cosets of H in $\mathbb{Z}_9$ are:

$$\begin{aligned}0 + H &= \{0, 3, 6\} = 3 + H = 6 + H\\ 1 + H &= \{1, 4, 7\} = 4 + H = 7 + H\\ 2 + H &= \{2, 5, 8\} = 5 + H = 8 + H.\end{aligned}$$

(iii) Let $G = D_4$ and $H = \{r_0, r_2\}$. The cosets of H in D_4 are:

$$\begin{aligned}r_0H &= \{r_0, r_2\} = H\\ r_1H &= \{r_1, r_1r_2\} = \{r_1, r_3\}\\ r_2H &= \{r_2, r_2r_2\} = \{r_2, r_0\} = H\\ r_3H &= \{r_3, r_3r_2\} = \{r_3, r_1\}\\ s_0H &= \{s_0, s_0r_2\} = \{s_0, s_2\}\\ s_1H &= \{s_1, s_1r_2\} = \{s_1, s_3\}\\ s_2H &= \{s_2, s_2r_2\} = \{s_2, s_0\}\\ s_3H &= \{s_3, s_3r_2\} = \{s_3, s_1\}\end{aligned}$$

In the example above, it is clear that cosets need not be subgroups, and that cosets of a subgroup H corresponding to different elements $a, b \in G$ can be the same.

Lemma 7.1.3. *Let H be a subgroup of G and let $a, b \in G$. Then*

(i) $a \in aH$.
(ii) $aH = H \iff a \in H$.
(iii) $(ab)H = a(bH)$ *and* $H(ab) = (Ha)b$.
(iv) $aH = bH \iff a \in bH$.
(v) $aH = bH$ *or* $aH \cap bH = \emptyset$.
(vi) $aH = bH \iff a^{-1}b \in H$.
(vii) $|\, aH \,| = |\, bH \,|$.
(viii) $aH = Ha \iff H = aHa^{-1}$.
(ix) aH *is a subgroup of* G *if and only if* $a \in H$.

Proof. (i) As H is a subgroup, $e \in H$ and so $a = ae \in aH$.

(ii) $a \in H$ implies that $ah \in H$ for each $h \in H$, so $aH \subseteq H$. On the other hand, $a \in H$ implies that $a^{-1} \in H$, so $h = a(a^{-1}h) \in aH$ for all $h \in H$, and hence $H \subseteq aH$. Conversely, suppose that $aH = H$. Then $a = ae \in aH = H$.

(iii) By associativity, $(ab)h = a(bh)$ and $h(ab) = (ha)b$ for all $h \in H$. Hence the given equalities of sets hold.

(iv) Suppose $aH = bH$. Then $a = ae \in aH = bH$. Conversely, suppose $a \in bH$. Then $a = bh_1$ for some $h_1 \in H$ and $aH = (bh_1)H = b(h_1H) = bH$ by parts (ii) and (iii).

(v) If $c \in aH \cap bH$, then by part (iv), $aH = cH = bH$.

(vi) $aH = bH$ if and only if $H = a^{-1}bH$, which by part (ii) holds if and only $a^{-1}b \in H$.

(vii) The map $ah \to bh$ from aH to bH is one-to-one and onto, and hence the two sets have the same cardinality.

(viii) $aH = Ha$ if and only if $aHa^{-1} = Haa^{-1} = H$.

(ix) If $a \in H$, then by part (ii), $aH = H$, which is of course a subgroup of G. Conversely, suppose aH is a subgroup. Then $e \in aH$ so that $eH \cap aH \neq \emptyset$. By part (v) $aH = eH = H$, so $a \in H$ by part (ii).

□

We note that properties (i), (v) and (vii) of Lemma 7.1.3 imply that a group G can be partitioned into distinct cosets of equal cardinality, and indeed the relation $a \sim b$ if and only if $aH = bH$ is an equivalence relation that partitions G into equivalence classes given by distinct cosets. The subgroup H is often thus chosen in such a way as to partition the group in some desirable way. For example, consider $H = SL(2, \mathbb{R}) \leq G = GL(2, \mathbb{R})$ and its cosets. For any matrix $A \in GL(2, \mathbb{R})$, the coset AH consists of all matrices with the same determinant as A (verify this!).

7.2. **Lagrange's Theorem.**

Theorem 7.2.1. *If G is a finite group and H is a subgroup of G, then $|\, H \,|$ divides $|\, G \,|$. The number of distinct left (right) cosets of H in G is $\frac{|\, G \,|}{|\, H \,|}$.*

Proof. Let $a_1H, \ldots, a_rH$ denote the distinct left cosets of H in G. Then for each $a \in G$, $aH = a_iH$ for some i, and $a \in aH = a_iH$. Thus each $a \in G$ belongs to a coset a_iH so that $G = a_1H \cup \ldots \cup a_rH$. This union is disjoint by part (v) of Lemma 7.1.3, hence $|\, G \,| = |\, a_1H \,| + \cdots + |\, a_rH \,| = r\,|\, H \,|$ (by part (vii) of Lemma 7.1.3). Hence $|\, H \,|$ divides $|\, G \,|$ and further, $\frac{|\, G \,|}{|\, H \,|}$ is equal to the number of left cosets of H in G.

□

Definition 7.2.2. The index of a subgroup H in G is the number of distinct left cosets of H in G, denoted by $|\, G : H \,|$.

A straightforward corollary of Lagrange's Theorem 7.2.1 is the following.

Corollary 7.2.3. *If G is a finite group and H is a subgroup of G, then $|G:H| = \frac{|G|}{|H|}$.*

Corollary 7.2.4. *In a finite group, the order of each element of the group divides the order of the group.*

Proof. Let G be a finite group and $a \in G$. Then $\langle a \rangle$, the cyclic subgroup generated by a, is a subgroup of G, hence $|a| = |\langle a \rangle|$ divides the order of G. □

Corollary 7.2.5. *A group of prime order is cyclic.*

Proof. Let G have prime order, say p and $e \neq a \in G$. Then by Lagrange's Theorem 7.2.1, $|\langle a \rangle|$ divides $|G| = p$, hence $|\langle a \rangle| = p$ or 1. As $a \neq e$, $\langle a \rangle$ must have order p, which implies that it is the whole group G. □

Corollary 7.2.6. *Let G be a finite group and let $a \in G$. Then $a^{|G|} = e$.*

Proof. By Corollary 7.2.4, there exists $n \in \mathbb{N}$ such that $n|a| = |G|$. Hence $a^{|G|} = a^{n|a|} = e$. □

Corollary 7.2.7 (Fermat's Little Theorem)**.** *For every integer a and every prime p, $a^p \mod p = a \mod p$.*

Proof. There exist integers m and r with $0 \leq r < p$ such that $a = pm + r$, that is, $a \mod p \equiv r$. So it suffices to prove that $r^p \mod p \equiv r$. If $r = 0$, the result is true. Assume that $r \in \{1, 2, \ldots, p-1\} = U(p)$. Then by Corollary 7.2.6, $r^{p-1} \mod p \equiv 1$. (We also showed this (Euler's Theorem) in Question 1 of Assignment 2.) Hence $r^p \mod p \equiv r$. □

Remark 7.2.8. The converse of Lagrange's theorem is false. Consider A_4 the alternating group of degree 4. Then $|A_4| = \frac{4!}{2} = 12$. But A_4 has no subgroups of order 6.

To see this, an easy computation gives that S_4 has 8 elements of order 3 and as they are all 3-cycles, they are even permutations and belong to A_4. Now, suppose that A_4 has a subgroup of order 6. Let a be an element of order 3 and suppose $a \notin H$. Then $A_4 = H \cup aH$ so that $a^2 \in H$ or $a^2 \in aH$. If $a^2 \in H$, then $a = a^4 \in H$, a contradiction. On the other hand, $a^2 \in aH$ implies that $a^2 = ah$ for some $h \in H$, so $a \in H$, a contradiction So it must be true that $a \in H$ for every a with order 3. But this implies that 8 elements belong to a subgroup of order 6, which is absurd.

This shows that unlike in a cyclic group, a finite group of order n need not have a subgroup of order k if k divides n (compare with Theorem 4.2.1).

Theorem 7.2.9. *For two finite subgroups H and K of a group, let $HK = \{hk \mid h \in H, k \in K\}$. Then $|HK| = \frac{|H||K|}{|H \cap K|}$*

Proof. On first glance, the set HK has $|H||K|$ products, but they may not all be distinct. That is, we may have $hk = h'k'$ with $h \neq h' \in H$ and $k \neq k' \in K$.

For each $t \in H \cap K$, $hk = h(tt^{-1})k = (ht)(t^{-1}k) \in HK$ as $ht \in H$ and $t^{-1}k \in K$. Hence each group element in HK is represented by at least $|H \cap K|$ products in HK. On the other hand, suppose $hk = h'k'$. Then $h'^{-1}h = k'k^{-1} = t \in H \cap K$, so $h = h't$ and $k = k't^{-1}$ with $t \in H \cap K$. Thus each element in HK is represented by exactly $|H \cap K|$ products, and $|HK| = \frac{|H||K|}{|H \cap K|}$. □

Example 7.2.10. A group of order 75 can have at most one subgroup of order 25. Suppose H, K are subgroups of order 25. Then as $H \cap K$ is a subgroup of H (or K), $|H \cap K|$ divides the

order of H (or K) so that $|\, H \cap K \,|$ is $1, 5$, or 25. The choices 1 and 5 lead to $|\, HK \,| = \frac{|\, H \,||\, K \,|}{|\, H \cap K \,|}$ equal to 625 and 125 respectively which gives a contradiction as the cardinality of HK must be less than or equal to the order of the group. Hence we must have $|\, H \cap K \,| = 25$, so that $H \cap K = H = K$.

Theorem 7.2.11 (Classification of Groups of order $2p$)**.** *Let G be a group of order $2p$, where p is a prime greater than 2. Then G is isomorphic to $\mathbb{Z}_{2p}$ or D_p.*

Proof. If G has an element a of order $2p$, then $G \cong \langle a \rangle$, that is, G is cyclic of order $2p$ and is isomorphic to $\mathbb{Z}_{2p}$ by Example 6.1.3 (iii).

If there is no element of order $2p$ in G, then by Corollary 7.2.4, any non-identity element of G must have order 2 or p. If every non-identity element of G has order 2, then G is Abelian (why?). In this case, the set $\{e, a, b, ab\}$ is closed and contains all inverses, hence it is a subgroup of order 4 of G, which is a contradiction as by Lagrange's theorem, any subgroup of G must have order 2 or p. Hence, some element $a \in G$ must have order p. Let $b \in G \setminus \langle a \rangle$. Then $|\, b \,| = 2$ or p. By another application of Lagrange's theorem, $|\, \langle a \rangle \cap \langle b \rangle \,|$ divides $|\, \langle a \rangle \,| = p$ and $\langle a \rangle \neq \langle b \rangle$ implies that $|\, \langle a \rangle \cap \langle b \rangle \,| = 1$. If $|\, b \,| = p$, then by Theorem 7.2.9, $|\, \langle a \rangle \langle b \rangle \,| = \frac{p^2}{1} = p^2 > 2p = |\, G \,|$, as $p > 2$. This is impossible, hence it must hold that $|\, b \,| = 2$. Thus, altogether, we have shown that any element outside $\langle a \rangle$ must have order 2. Further, note that $e, a, a^2, \ldots, a^{p-1}$ and $b, ab, a^2b, \ldots, a^{p-1}b$ are all distinct elements of G. Since there are $2p$ such elements and $|\, G \,| = 2p$, they must be all the elements of G.

Consider the element ab. As it does not belong to $\langle a \rangle$, it must have order 2. Hence $ab = (ab)^{-1} = ba^{-1}$. This relation will determine the multiplication table of G.

Recall the dihedral group D_p of order $2p$ for $p \geq 3$. Choose a rotation of order p (for example r_1) and any reflection (say, s_2). Then every element of D_{2p} can be written as products of these two elements (verify this!). The set $\{r_1, s_2\}$ is said to *generate* the group G. Further, $r_1 s_2 = s_3$ and $s_2 r_1^{-1} = s_2 r_{p-1} = s_{2-p+1 \mod p} = s_3$ so that $r_1 s_2 = s_2 r_1^{-1}$.

In G (and D_p), the multiplication table is completely determined by the relation $ab = ba^{-1}$ as we have the following:

$$a^k a^l = a^{k+l \bmod p}, \quad a^k (a^l b) = a^{k+l \bmod p} b,$$
$$(a^l b) a^k = b a^{-l} a^k = b a^{k-l \bmod p} = a^{l-k \bmod p} b, \quad (a^k b)(a^l b) = a^k b^2 a^{-l} = a^{k-l \bmod p}$$

Hence $G \cong D_p$ via the isomorphism $\varphi(a^q b^r) = r_1^q s_2^r$, $q = 0, \ldots, p-1$ and $r = 0, 1$. □

Corollary 7.2.12. *The group S_3 is isomorphic to D_3.*

Proof. The group S_3 is of order $6 = 2(3)$ and it is not cyclic. Hence it must be isomorphic to D_3 by Theorem 7.2.11. □

7.3. **An application to permutation groups.**

Definition 7.3.1. Let G be a group of permutations of a set S. For each $i \in S$, let $\mathrm{stab}_G(i) = \{\varphi \in G \mid \varphi(i) = i\}$. The set $\mathrm{stab}_G(i)$ is called the stabilizer of i in G.

Exercise 7.3.2. $\mathrm{stab}_G(i)$ is a subgroup of G.

Definition 7.3.3. Let G be a group of permutations of a set S. For each $i \in S$, let $\mathrm{orb}_G(i) = \{\varphi(i) \mid \varphi \in G\}$. The set $\mathrm{orb}_G(i)$ is a subset of S called the orbit of i under G.

Example 7.3.4. Let the group G be given by

$$G = \{(1), (1,3,2)(4,6,5)(7,8), (1,3,2)(4,6,5), (1,2,3)(4,5,6), (1,2,3)(4,5,6)(7,8), (7,8)\}.$$

Then

$$\begin{array}{llll} \mathrm{orb}_G(1) & = \{1,3,2\} & \mathrm{stab}_G(1) & = \{(1),(7,8)\} \\ \mathrm{orb}_G(2) & = \{2,1,3\} & \mathrm{stab}_G(2) & = \{(1),(7,8)\} \\ \mathrm{orb}_G(3) & = \{3,2,1\} & \mathrm{stab}_G(3) & = \{(1),(7,8)\} \\ \mathrm{orb}_G(4) & = \{4,6,5\} & \mathrm{stab}_G(4) & = \{(1),(7,8)\} \\ \mathrm{orb}_G(5) & = \{5,4,6\} & \mathrm{stab}_G(5) & = \{(1),(7,8)\} \\ \mathrm{orb}_G(6) & = \{6,5,4\} & \mathrm{stab}_G(6) & = \{(1),(7,8)\} \\ \mathrm{orb}_G(7) & = \{7,8\} & \mathrm{stab}_G(7) & = \{(1),(1,3,2)(4,6,5),(1,2,3)(4,5,6)\} \\ \mathrm{orb}_G(8) & = \{8,7\} & \mathrm{stab}_G(8) & = \{(1),(1,3,2)(4,6,5),(1,2,3)(4,5,6)\} \end{array}$$

Theorem 7.3.5 (Orbit Stabilizer)**.** *Let G be a finite group of permutations of a set S. Then for any $i \in S$, $|\,G\,| = |\,\mathrm{orb}_G(i)\,|\,|\,\mathrm{stab}_G(i)\,|$.*

Proof. We know by Lagrange's theorem that $\frac{|\,G\,|}{|\,\mathrm{stab}_G(i)\,|}$ gives the number of left cosets of $\mathrm{stab}_G(i)$ in G. We will give a one-to-one correspondence between the left cosets of $\mathrm{stab}_G(i)$ and the elements in the orbit of i.

Define $T(\varphi\,\mathrm{stab}_G(i)) = \varphi(i)$. To see that T is well-defined, note that if $\alpha\,\mathrm{stab}_G(i) = \beta\,\mathrm{stab}_G(i)$, then $\alpha^{-1}\beta \in \mathrm{stab}_G(i)$ so that $(\alpha^{-1}\beta)(i) = i$. This gives that $\alpha(i) = \beta(i)$, so T is well defined.

Next we show that T is one-to-one. Suppose $\alpha(i) = \beta(i)$, then $(\alpha^{-1}\beta)(i) = i$, so $\alpha^{-1}\beta \in \mathrm{stab}_G(i)$. This implies that $\alpha\,\mathrm{stab}_G(i) = \beta\,\mathrm{stab}_G(i)$ establishing that T is one-to-one.

Finally we show that T is onto. Let $j \in \mathrm{orb}_G(i)$, then $j = \alpha(i)$ for some $\alpha \in G$. Hence $j = \alpha(i) = T(\alpha\,\mathrm{stab}_G(i))$.

Altogether, we have shown that there exists a bijection between the left cosets of $\mathrm{stab}_G(i)$ and the orbit of i, hence $\frac{|\,G\,|}{|\,\mathrm{stab}_G(i)\,|} = |\,\mathrm{orb}_G(i)\,|$. □

7.4. **Rotation group of a cube.**

Example 7.4.1. Let G be the rotation group of a cube. What is $|\,G\,|$? We can view G as a group of permutations on the set $\{1,2,3,4,5,6\}$ as any rotation must carry a face of the cube to a face of the cube.

Let us fix the face corresponding to 1, say and use the Orbit-Stabilizer theorem. There exists a rotation that carries face 1 to each of the faces $1,2,3,4,5,6$, hence $|\,\mathrm{orb}_G(i)\,| = 6$. The rotations that fix face 1 are given by rotations of $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ about the line perpendicular to face 1 passing through the center of the cube. Hence $|\,\mathrm{stab}_G(i)\,| = 4$. Altogether, $|\,G\,| = |\,\mathrm{orb}_G(1)\,|\,|\,\mathrm{stab}_G(1)\,| = 6 \times 4 = 24$.

Theorem 7.4.2. *The group of rotations of a cube is isomorphic to S_4.*

Proof. We proved in the example above that $|\,G\,| = 24$. We will show that G maps to a subgroup of S_4, hence must be equal to S_4 as it has the same cardinality.

To each rotation of the cube, we associate an element of S_4. In particular, a cube has 4 diagonals and the rotation group induces a group of permutations on the four diagonals. Labelling the diagonals a, b, c, d, we see that there is a $\frac{\pi}{2}$ rotation that yields the permutation $\alpha = (1,2,3,4)$ (see figure 1 below) and a $\frac{\pi}{2}$ rotation that yields $\beta = (1,4,2,3)$.

Hence the group of permutations of the diagonals induced by the rotations of the cube contains the 8 element subgroup $\{\varepsilon, \alpha, \alpha^2, \alpha^3, \beta^2, \beta^2\alpha, \beta^2\alpha^2, \beta^2\alpha^3\}$ and also the element $\alpha\beta$ which has order 3. Hence the order of the group of permutations of the diagonals induced by the rotations of the cube is a multiple of 8 and 3, hence must be 24. Hence $G \cong S_4$. □

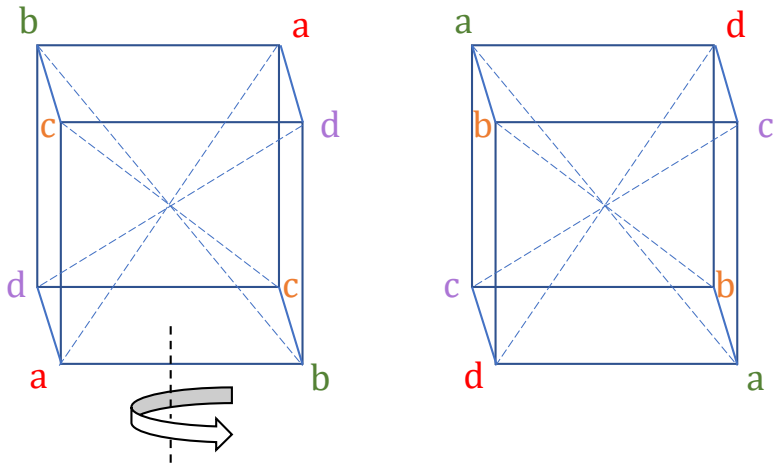

FIGURE 1. The rotation yielding the permutation α

REFERENCES

[1] Chapter 7. Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.