Advanced Algebra I Lecture Notes

Aleck Zhao

October 5, 2016

This is AS.110.401 Advanced Algebra I, taught by Caterina Consani.

Contents

1 26 September, 2016

1.1 Subgroups

Goal: Find subsets of a given group which inherit the same law as the group itself.

Example

Some examples of a chain of subsets.

- $\{\pm 1\} \subset \{\pm 1, \pm i\} \subset \mathbb{C}^0 = \{z \in \mathbb{C}^* \big| |z| = 1\} \subset \mathbb{C}^*$
- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset (\mathbb{C}, +)$
- $A_n \subset (S_n, \circ)$

Definition. $H \subset G$ where G is a group, is a subgroup of G if H is a group with respect to the same operation for G.

Theorem (Subgroup Test)

A subset $H \subset G$ is a subgroup if:

1. $1_G \in H$
2. $h, h' \in H \implies hh' \in H$
3. $h \in H \implies h^{-1} \in H$ (where $h \in G$ is the inverse of h)

Proof.

1. Let $e \in H$ be the identify of H. Then $e^2 = e = e \cdot 1_G$, then by the cancellation law in G it follows that $e = 1_G$.
2. This follows from the fact that H is a subgroup, so it is closed under the operation.
3. Let $h \in H$ and $h' \in H$ be its inverse. If $h^{-1} \in G$ is the inverse of h in G, then $hh' = 1 = hh^{-1} \implies h' = h^{-1}$ by the cancellation law in G.

□

Example

$n\mathbb{Z} \subset \mathbb{Z}$ is a subgroup for fixed n.

Theorem (Finite group test)

If $|H| < \infty$, $H \neq \{\}$, and $H \subset G$ group. Then H is a subgroup if and only if H is closed.

Proof. H is closed and finite. Let $h \in H$ such that $h^n = h^{m+n}$ for some $m, n \geq 1$. Then by the cancellation in G, this means $1_G = h^m$, so $1_G \in H$. Then since $1_G = h^{m-1}h$, so $h^{-1} = h^{m-1} \in H$. □

Example

Consider $G = \mathbb{Z}_3$, study its subgroups. Trivially the sets $H_1 = \{\bar{0}\}$ and $H_2 = \mathbb{Z}_3$ are subgroups. Does there exist a subgroup of $\mathbb{Z}_3$ with cardinality 2?

Consider the possible sets H_3. If $H_3 = \{\bar{0}, \bar{1}\}$ then H_3 is not closed wince $\bar{1} + \bar{1} = \bar{2} \notin H_3$. Similarly for other combinations.

An element g is a **generator** if all elements of G can be generated by g.

Example

$\mathbb{Z}_3 = \{n \cdot \bar{1} | \, n \in \mathbb{Z}\}$ so $\bar{1}$ is a generator for $\mathbb{Z}_3$.

Example (Groups of order 4)

Let $|G| = 4$. From the Cayley table, we know that

$$G = \begin{cases} \mathbb{Z}_4 \\ K_4 \end{cases}$$

where K_4 is the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

In the first case, $G = \{1, a, a^2, a^3\}$ such that $a^4 = 1$. A trivial subgroup is $H_1 = \{1\}$. If $|H| = 2$, then $H_2 = \{1, x\}$ where $x^2 \in H_2$, thus it must be that $H_2 = \{1, a^2\}$. We can't have $x = a$ or $x = a^3$ because a^2 would not be in H_2, and because $(a^3)^2 = a^6 = a^2$ would not be in H_2. Similarly we can't have $|H_3| = 3$, so the only subgroups are $\{1\}, \{1, a^2\}, G$.

In the second case, $G = \{1, a, b, c\}$ such that $a^2 = b^2 = c^2 = 1$. Then $H_2 = \{1, a\}$ and similarly $\{1, b\}$ and $\{1, c\}$ are all subgroups. There are no subgroups of size 3 because elements such as ab and bc would not be contained, so they would not be closed. Thus, the subgroups are $\{1\}, \{1, a\}, \{1, b\}, \{1, c\}, G$.

Example

If $|G| = 6$, then either G is commutative or $G = S_3 = \left\{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\right\}$ with the identities $\sigma^3 = \tau^2 = \varepsilon$ and $\sigma\tau\sigma = \tau$. Then the subgroups are

$$\begin{aligned} H_1 &= \{\varepsilon\} \\ H_2 &= \{\varepsilon, \tau\} \\ H_3 &= \{\varepsilon, \tau\sigma\} \\ H_4 &= \left\{\varepsilon, \tau\sigma^2\right\} \\ H_5 &= \left\{\varepsilon, \sigma, \sigma^2\right\} \\ H_6 &= S_3 \end{aligned}$$

On the other hand, if G is commutative, then $G = \mathbb{Z}_6$. Then the subgroups are

$$\begin{aligned} H_1 &= \{1\} \\ H_2 &= \{0, 3\} \\ H_3 &= \{0, 2, 4\} \\ H_4 &= \mathbb{Z}_6 \end{aligned}$$

so these clearly have different group structures.

Remark. The cardinality of the subgroups divide the cardinality of the whole group. Coincidence?

Remark. We stated without proof that $\mathbb{Z}_6$ is the only commutative group of order 6 (up to isomorphism).

Definition. The subgroup of **centers** of G is defined as

$$Z(G) := \{z \in G |\, gz = zg, \forall g \in G\}$$

If G is commutative, then $Z(G) \equiv G$. On the other hand if G is not commutative, then $Z(G)$ can be very small.

Example

Proof in book. $Z(S_n) = \{\varepsilon\}$

Example

$|G| = 8$ where G is non-commutative. An example is the group of **quaternions** which is defined as

$$G = Q := \{\pm 1, \pm i, \pm j, \pm k\}$$

such that

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ ij = -ji &= k \\ jk = -kj &= i \\ ki = -ik &= j \end{aligned}$$

Q can be realized as a subgroup of $\mathrm{GL}_n(\mathbb{C})$. Then the subgroup of centers is $Z(Q) = \{\pm 1\}$, so Q is very non-commutative.

Theorem

If G is a group and $H, K \subset H$ are subgroups, then

1. $H \cap K := \{g \in G |\, g \in H, g \in K\}$ is a subgroup of G
2. $\forall g \in G$, the set $gHg^{-1} := \left\{ghg^{-1} |\, h \in H\right\}$ is a subgroup of G. The group gHg^{-1} is called a **conjugate** of H in G.

Fact. $|H| = |gHg^{-1}|$ if H is finite.

Fact. If G is commutative, then $gHg^{-1} \equiv H$.

2 5 October, 2016

2.1 Cosets

Suppose G is a group and $H \subset G$ is a subgroup of G. Then for some $a \in G$, the set

$$Ha := \{ha | h \in H\}$$

is the **right coset** generated by a. Similarly, the set

$$aH := \{ah | h \in H\}$$

is the **left coset** generated by a.

Example

Let $4\mathbb{Z} \subset \mathbb{Z}$, then since $\mathbb{Z}$ is commutative, the left and right cosets are the same, and they are

$$1 + 4\mathbb{Z}, \quad 2 + 4\mathbb{Z}, \quad 3 + 4\mathbb{Z}, \quad 4\mathbb{Z}.$$

Remark 2.1. If G is abelian, then $aH = Ha$ for all $a \in G$.

Theorem

Let G be a group, $H \subset G$ is a subgroup, and let $a, b \in G$.

(1) $H = H \cdot 1 = 1 \cdot H$

(2) $aH = H \iff a \in H$

(3) $Ha = Hb \iff ab^{-1} \in H$

(4) $a \in Hb \implies Ha = Hb$

(5) $Ha = Hb$ or $Ha \cap Hb = \{\}$

(6) $G = \coprod\limits_{a \in G} Ha$ is a partition of G.

Remark 2.2. (5) and (6) are very similar to properties of equivalence classes on a set.

Proof. Proof of (3): $Ha = Hb \implies a \in Ha = Hb$ so $a \in Hb$ so a can be written as $a = hb$ for some $h \in H$, so right multiplying by b^{-1}, we have $ab^{-1} = h \in H$ as desired.

For the reverse direction if $ab^{-1} \in H$, then $ha = h(ab^{-1})b \in Hb$ since $h, ab^{-1} \in H \implies h(ab^{-1}) \in H$ thus since $ha \in Ha$ belongs to Hb, we have $Ha \subset Hb$. Then $b^{-1}a = (ab^{-1})^{-1} \in H$ so $hb = h(ba^{-1})a \in Ha$ so $Hb \subset Ha$ so in fact $Ha = Hb$.

(3) $\implies$ (2) by choosing $b = 1$.

Proof of (5): If $Ha \cap Hb \neq \{\}$, then there must be an element in common. Let $x \in Ha \cap Hb$ be this element, then $x \in Ha$ so $Hx = Ha$ and $Hx = Hb$ so $Ha = Hb$. $\square$

Example 2.3

Let $G = \langle a \rangle$ be a group, where $o(a) = 4$ so $G = \{1, a, a^2, a^3\}$. Find the cosets of $H = \langle a^2 \rangle = \{1, a^2\}$.

Since $a^2 \in H$, then $Ha^2 = H$. Next, $Ha = \{a, a^3\}$ and notice $Ha \cap H = \{\}$. Then G is partitioned by $H \cdot 1$ and Ha and $|H| = |Ha|$.

Lemma 2.4

Let G be a group and $H \subset G$ be a subgroup.

(1) $|H| = |Ha| = |aH|$ for all $a \in G$.

(2) $\varphi : \{Ha | a \in G\} \to \{bH | b \in G\}$ where $\varphi(Ha) = a^{-1}H$ is a bijection of sets.

Proof. For (1): $|H| = |Ha|$ since $h \mapsto ha$ defines a bijection. This map is injective since if $h_1 a = ha$ then $h_1 = h$ by the cancellation law, and surjective because for all $ha \in Ha$ we can recover the $h \in H$ such that $h \mapsto ha$. Thus $|H| = |Ha|$. □

Remark 2.5. The sets of right and left cosets for the same $H \subset G$ have the same cardinality.

Definition 2.6. $|G : H|$ is the **index** of H in G and is defined as the cardinality of the set $\{Ha | a \in G\}$.

Remark 2.7. This applies even for infinite sets, for example $|\mathbb{Z} : 4\mathbb{Z}| = 4$.

Theorem 2.8 (Langrange's Theorem)

Let G be a group and $H \subset G$ is a subgroup, and $|G|$ is finite.

(1) $|H| \,\big|\, |G|$

(2) $|G : H| = \dfrac{|G|}{|H|}$

Proof. For (1): Let $k = |G : H|$ where the set of right cosets is $\{Ha_1, Ha_2, \cdots, Ha_k\}$ where $a_i \in G$. Then

$$G = Ha_1 \sqcup Ha_2 \sqcup \cdots \sqcup Ha_k$$

and since these are disjoint sets, the cardinality of G is the sum of the cardinalities of the cosets, which are all $|H|$ since $|H| = |Ha|$, so $|G| = k|H|$. □

Corollary 2.9

If $|G|$ is finite, and $g \in G$, then $o(g) = |\langle g \rangle| \,\big|\, |G|$.

Remark 2.10. The converse of Lagrange's Theorem fails in general.

Example 2.11

Take $A_4 \subset S_4$ the subgroup of even permutations. Then $|A_4| = |S_4|/2 = 12$, but there does not exist a subgroup $H \subset A_4$ such that $|H| = 6$.

Indeed $K_4 = \{\varepsilon, (12)(34), (13)(24), (14)(23)\}$ is a subgroup of A_4 and let $H = \langle\sigma\rangle = \langle(123)\rangle$ be the group generated by the 3-cycles. Then $|H| = 3, |K_4| = 4$ and the Cartesian product

$$H \times K_4 = \{hk | h \in H, k \in K_4\}$$

is a group of order 12. However, note that $\forall\gamma \in K_4$ and $\forall\sigma' \in H$, the order

$$o(\gamma\sigma') = \begin{cases} 1 \\ 2 \\ 3 \end{cases}$$

so there is no element $g \in A_4$ such that $o(g) = 6$ so there does not exist a subgroup $G \subset A_4$ such that $|G| = 6$.

2.2 Normal Subgroups

Definition 2.12. Given a group G, a subgroup $H \subset G$ is said to be **normal** if $aH = Ha, \forall a \in G$.

Example 2.13 (non-example)

$G = S_3$ and take $H = \{\varepsilon, \tau\}$ where $\tau^2 = \varepsilon$ and let $\sigma \in S_3$ such that $\sigma^3 = \varepsilon$. Then $\sigma H \neq H\sigma$.

¡++¿