Introduction to Some of Group Theory

Steven Miller*

Abstract

We will review some group theory.

1 Lagrange's Theorem

1.1 Basic group theory

Group G is a set of elements g_i satisfying the four conditions below, relative to some binary operation. We often use multiplicative notation $(g_1 g_2)$ or additive notation $(g_1 + g_2)$ to represent the binary operation. For definiteness, we use multiplicative notation below; however, one could replace xy with $b(x, y)$ below.

If the elements of G satisfy the following four properties, then G is a group.

1. $\exists e \in G$ s.t. $\forall g \in G : eg = ge = g$. (Identity.) We often write $e = 1$ for multiplicative groups, and $e = 0$ for additive groups.
2. $\forall x, y, z \in G : (xy)z = x(yz)$. (Associativity.)
3. $\forall x \in G, \exists y \in G$ s.t. $xy = yx = e$. (Inverse.) We write $y = x^{-1}$ for multiplication, $y = -x$ for addition.
4. $\forall x, y \in G : xy \in G$. (Closure.)

*E-mail: `millerj@cims.nyu.edu` or `sjmiller@math.princeton.edu`

If commutation holds ($\forall x, y \in G$, $xy = yx$), we say the group is Abelian. Non-abelian groups exist and are important. For example, consider the group of $N \times N$ matrices with real entries and non-zero determinant. Prove this is a group under matrix multiplication, and show this group is not commutative.

H is a *subgroup* of G if it is a group and its elements form a subset of those of G. The identity of H is the same as the identity of G. Once you've shown the elements of H are closed (ie, under the binary operation, $b(x, y) \in H$ if $x, y \in H$), then associativity in H follows from closure in H and associativity in G.

For the application to Fermat's Little Theorem you will need to know that the set $\{1, x, x^2, \cdots x^{n-1}\}$ where n is the lowest positive integer s.t. $x^n = 1$, called the *cyclic group*, is indeed a subgroup of any group G containing x, as well as n divides the order of G.

For a nice introduction to group theory see: M. Tinkham, *Group Theory and Quantum Mechanics*, (McGraw-Hill, 1964) or S. Lang, *Undergraduate Algebra*.

1.2 Lagrange's Theorem

The theorem states that if H is a subgroup of G then $|H|$ divides $|G|$.

First show that the set hH, *i.e.* all the elements of H premultiplied by one element, is just H rearranged (Cayley's theorem). By closure hH falls within H. We only need to show that hh_i can never equal hh_j for two different elements $i \neq j$. If it were true, since a unique h^{-1} exists we could premultiply the equation $hh_i = hh_j$ by h^{-1} to give $h_i = h_j$, which is false. Therefore $hh_i \neq hh_j$, and we have guaranteed a 1-to-1 mapping from H to hH, so $hH = H$.

Next we show that the sets g_iH and g_jH must either be completely disjoint, or identical. Assume there is some element in both. Then $g_ih_1 = g_jh_2$. Multiplying on the right by $h_i^{-1} \in H$ (since H is a subgroup) gives $g_i = g_jh_2h_1^{-1}$. As H is a subgroup, $\exists h_3 \in H$ such that $h = h_2h_1^{-1}$. Thus $g_i = g_jh_3$. Therefore, as $h_3H = H$, $g_iH = g_jh_3H = g_jH$, and we see if the two sets have one element in common, they are identical. We call a set gH a *coset* (actually, a left coset) of H.

Clearly

$$G = \bigcup_{g \in G} gH \tag{1}$$

Why do we have an equality? As $g \in G$ and $H \subset G$, every set on the right is contained in G. Further, as $e \in H$, given $g \in G$, $g \in gH$. Thus, G is a subset of the right side, proving equality.

There are only finitely many elements in G. As we go through all g in G, we see if the set gH equals one of the sets already in our list (recall we've shown two cosets are either identical or disjoint). If the set equals something already on our list, we do not include it; if it is new, we do. Continuing this process, we obtain

$$G = \bigcup_{i=1}^{k} g_i H \tag{2}$$

for some finite k. If $H = \{e\}$, k is the number of elements of G; in general, however, k will be smaller.

Each set $g_i H$ has $|H|$ elements. Thus, $|G| = k|H|$, proving $|H|$ divides $|G|$.

2 Quotient groups

Say we have a finite Abelian group G (this means for all $x, y \in G$, $xy = yx$) of order m which has a subgroup H of order r. We will use multiplication as our group operation. Recall the *coset* of an element $g \in G$ is defined as the set of elements $gH = g\{h_1, h_2, \cdots, h_r\}$. Since G is Abelian (commutative) then $gH = Hg$ and we will make no distinction between left and right cosets here.

The *quotient group* (or *factor group*), symbolized by G/H, is the group formed from the cosets of all elements $g \in G$. We treat each coset $g_i H$ as an element, and define the multiplication operation as usual as $g_i H g_j H$. Why do we need G to be Abelian? The reason is we can then analyze $g_i H g_j H$, seeing that it equals $g_i g_j HH$. We will analyze this further when we prove that the set of cosets is a group.

There are several important facts to note. First, if G is not Abelian, then the set of cosets might not be a group. Second, recall we proved the coset decomposition rule: given a finite group G (with n elements) and a subgroup H (with r elements) then there exist elements g_1 through g_k such that

$$G = \bigcup_{i=1}^{k} g_i H. \tag{3}$$

The choices for the g_i's is clearly not unique. If g_1 through g_k work, so do $g_1 h_1$ through $g_k h_k$, where h_i is any element of H. Recall this was proved by showing any two cosets are either distinct or identical.

We will show below that, for G Abelian, the set of cosets is a group. Note, however, that while it might at first appear that there are many different ways to write the coset group, they really are the same. For example, the cosets gH and $gh_1 h_2^4 h_3 H$ are equal. This is similar to looking at integers mod n; mod 12, the integers 5, -7 and 19 are all equal, even though they look different.

We now prove that the set of cosets is a group (for G Abelian).

Closure. By commutivity $g_i H g_j H = g_i g_j HH$. What is "HH"? Just the set of all r^2 possible combinations of elements of H. By closure, and the existence of the identity, this just gives H again (recall no element in a group can appear more than once—duplicates are removed). Therefore $g_i H g_j H = g_i g_j H$. Now, as G is a group and is closed, $g_i g_j \in G$. Thus, there is a α such that $g_i g_j \in g_\alpha H$ (as $G = \bigcup_{\beta=1}^{k} g_\beta H$. Therefore, there is an $h \in H$ such that $g_i g_j = g_\alpha h$, which implies $g_i g_j H = g_\alpha h H = g_\alpha H$. Thus, the set of cosets is closed under coset multiplication. Note, however, that while the coset $g_i g_j H$ is in our set of cosets, it may be written differently.

Identity. If e is identity of G, then $eHg_i H = g_i H$ and $g_i HeH = g_i H$, so eH is the identity of this quotient group.

Associativity. Since as you may have noticed, the quotient group elements behave just like those of G, associativity follows from that of G.

Inverse. It is easy to guess $g^{-1}H$ is the inverse of gH. Check it: $g^{-1}HgH = g^{-1}gH = eH =$ identity, also true the other way round of course by commutativity. Unfortunately, $g^{-1}H$ might not be listed as one of our cosets! Thus, we must be a little more careful. Fortunately, as $g^{-1} \in G = \bigcup_{\beta=1}^{k} g_\beta H$, there is an α such that $g^{-1} \in g_\alpha H$. Then, there is an $h \in H$ with $g^{-1} = g_\alpha h$. Thus, $g^{-1} = g_\alpha h H = g_\alpha H$, and direct calculation will show that the coset $g_\alpha H$ is the inverse (under coset multiplication) of gH.