Math 220A: Part 1.1

The Definition and Basic Examples

This is course on group theory. We assume you are familiar with groups from a prior course so we will move quickly through the basics. For the first few sessions we will establish notation and look at a number of examples. We will also set a perspective we want utilize throughout the course, namely we want to consistently think about group actions, not just groups in isolation. More on that in a bit. First the definition.

Definition G1. A group is a set G together with a binary operation $\cdot : G \times G \to G$ satisfying the following conditions:
G1: (Associativity) for all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
G2: (Identity Element) There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$;
G3: (Inverses) For each $a \in G$, there exists an $a^{-1} \in G$ such that $a \cdot a^{-1} = e \in G$ and $a^{-1} \cdot a = e \in G$.
We usually abbreviate $(G, \cdot)$ simply by G where the operation is implicit and the notation for the operation may vary according to context and the conventional use (it could be $+$, $\cdot$, $\times$, $\circ$, or nothing (concatenation) which are the most common.) In class I tend use notation that makes sense and may not always define it–but don't be shy to ask if there is any confusion.

There are examples you know very well. I'll write them down here without discussing them (yet): $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ $(\mathbb{R} - \{0\}, \cdot)$, $(\mathbb{C} - \{0\}, \cdot)$, $(\mathbb{Z}/n\mathbb{Z}, +)$ and when p is prime $(\mathbb{Z}/p\mathbb{Z} - \{0\}, \cdot)$. Of course all these are commutative.The first non commutative groups you encountered were the general linear groups $\mathrm{GL}_n(\mathbb{R})$ (invertible $n \times n$ matrices) or possibly the symmetric groups S_n, which will be discussed more shortly.

Prior to looking at more examples here is some basic terminology:

If $xy = yx$ for all $x, y \in G$ then G is called *commutative* or *abelian*.

If G is finite then the number of elements in G is called the *order* of G, usually denoted $|G|$.

A subgroup of $H \subseteq G$ is as expected, it is a subset which is closed under the group operation and inverses.

Non Commutative Examples. Probably the most basic non commutative groups are the general linear groups and their subgroups. These are

the groups of invertible matrices with coefficients in a some (commutative) ring or field. (We will use familiar rings and fields.) The fact that invertible matrices over a commutative ring form a group follows from basic linear algebra.

Specifically $\mathrm{GL}_n(R)$ where R is a ring is the group of invertible $n \times n$ matrices. Common examples are where $R = \mathbb{R}, \mathbb{C}, \mathbb{Z}$, or $\mathbb{Z}/n\mathbb{Z}$. Because finite groups are good examples in introductory courses and because linear algebra is a convenient tool to use when looking at $\mathrm{GL}_n(R)$ we also will be interested the case where R is the finite field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ where p is prime.

As a nice exercise, and as a warm-up for our discussion of group actions, compute the number of elements in $\mathrm{GL}_2(\mathbb{F}_p)$. Here is a hint: The elements of $\mathrm{GL}_2(\mathbb{F}_p)$ are in one-to-one correspondence with all the linear isomorphisms $\mathbb{F}_p^2 \to \mathbb{F}_p^2$ (with respect to some basis, which might as well be the standard basis.) If you recall the process $T : \mathbb{F}_p^2 \to \mathbb{F}_p^2$ for obtaining the matrix A associated with a linear transformation (some texts might write $T = T_A$) you will remember that the first column of A is the image of the first basis vector and the second column is the image of the second basis vector. So, since T is invertible, and as $\mathbb{F}_p^2$ has p^2 elements, we see there are p^2-1 choices for the first column of A (it can't be zero) and then there are $p^2 - p$ choices for the second column of A (it can't be a multiple of the first). Therefore $\mathrm{GL}_2(\mathbb{F}_p)$ has $(p^2-1)(p^2-p)$ elements. I leave it to you to generalize this to the case of $\mathrm{GL}_n(\mathbb{F}_p)$. Similar reasoning will be used when subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$ are analyzed. The comment about the argument just given is that we are thinking about the group as acting on the $\mathbb{F}_p$-vector space $\mathbb{F}_p^2$ in the analysis. Whenever you can think of a group as acting on a set (we will discuss this shortly) it provides a good way to get a handle on the structure of the group.

Basic Properties of Groups

We next give some basic properties of groups. They are typically covered in undergraduate Abstract Algebra courses. They are not going to be proved here; what I suggest is that you read them through, write out one or two proofs carefully, and ask if you have any questions.

Group Property G2a. The identity element in a group G is unique; that is, there exists only one element $e \in G$ such that G2 holds.

Group Property G2b. If g is any element in a group G, then the inverse of g, denoted by g^{-1}, is unique.

Group Property G2c. Let G be a group. If $a, b \in G$, then $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Group Property G2d. Let G be a group. For any $a \in G$, $(a^{-1})^{-1} = a$.

Group Property G2e. Let G be a group. If $a, b \in G$, then the equations $ax = b$ and $xa = b$ have unique solutions in G.

Group Property G2f. If G is a group and $a, b, c \in G$, then $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

Group Property G2g. In a group, the usual laws of exponents hold; that is, for all $g, h \in G$,
1. $g^m g^n = g^{m+n}$ for all $m, n \in \mathbb{Z}$;
2. $(g^m)^n = g^{mn}$ for all $m, n \in \mathbb{Z}$;
3. Furthermore, if G is commutative, then $(gh)^n = g^n h^n$.

More Examples.

We continue with more examples.

Examples 2. Let X be a set and then let $S(X)$ denote the set of all bijective functions $X \to X$, that is $S = \{f : X \to X | f \text{ is bijective } \}$. Let $\circ$ denote composition of functions. Then $(S(X), \circ)$ is a group, called the group of permutations of X. Since function composition is associative (incidentally that is one way to see why matrix multiplication is associative) it is clear that $(S(X), \circ)$ is a group.

The familiar case is $S_n := S(\{1, 2, \ldots, n\})$, the group of permutation on $\{1, 2. \ldots, n\}$. The customary notation for elements of S_n is to represent them as products of disjoint cycles. There is a theorem embedded in this representation (namely that every element has such a form) which will be sketched shortly, but because the notation is so convenient and we want to consider this example, we introduce it here.

• A r-cycle $f \in S_n$ for $2 \leq r \leq n$ is an element for which there are r distinct elements $\{i_1, i_2, \ldots i_r\} \subseteq \{1, 2. \ldots, n\}$ for which $f(i_1) = i_2$, $f(i_2) = i_3$,$\ldots f(i_{r-1}) = i_r$, $f(i_r) = i_1$, and for which $f(j) = j$ for all $j \in \{1, 2. \ldots, n\} - \{i_1, i_2, \ldots i_r\}$. In this case we use the notation $f = (i_1, i_2, i_3, \ldots i_r)$. Note that this notation is not unique, for $(i_1, i_2, i_3, \ldots i_r) = (i_2, i_3, \ldots i_r, i_1)$, and so forth.

• Two cycles $(i_1, i_2, i_3, \ldots i_r)$ and $(j_1, j_2, j_3, \ldots i_s)$ are said to be *disjoint* if $\{i_1, i_2, i_3, \ldots i_r\} \cap \{j_1, j_2, j_3, \ldots j_s\} = \emptyset$.

• If two cycles $f = (i_1, i_2, i_3, \ldots i_r)$ and $g = (j_1, j_2, j_3, \ldots j_s)$ are disjoint then $f \circ g = g \circ f$.

The theorem that gives a crucial representation for elements of S_n is the following.

Theorem G3. (Disjoint Cycle Representations) Every element $f \in S_n$ can be expressed $f = f_1 f_2 \cdots f_t$ where each f_ℓ is a cycle and these t cycles are pairwise disjoint. Moreover this product is uniquely determined up to the order of the cycles.

The proof sketch is as follows. If $f \in S_n$, start somewhere and consider iterations of applications of f from that starting point. Eventually you get back to where you started and you have a first cycle in the product. Now start somewhere not yet listed and consider iterations of applications of f from that starting point until you get back to where you started. That gives another cycle it the product. Keep doing this, where if you have a fixed point x (so $f(x) = x$) you add that element to the list without it appearing in a cycle. After you have exhausted all possible elements of $\{1, 2, \ldots, n\}$ (either as part of a cycle or as a fixed point) you are done. Of course you have to check that the cycles you get are disjoint, and uniquely determine a partition of $\{1, 2, \ldots, n\}$ (one subset for each cycle and a final subset of fixed points), but that not hard.

In order to illustrate the result (and its proof) we show how the cycle notation can be used to calculate products. Consider $f = (13)(246)$, $g = (1352) \in S_6$. Then we can compute the product $fg := f \circ g$. Keep in mind that the way we have set up notation, the products are function composition so you start on the right and go to the left to find product. Doing this we find

$$fg = (13)(246)(1352) = (1)(23546) = (23546).$$

Verbally what we are doing is this: we note $1 \mapsto 3 \mapsto 3 \mapsto 1$ by starting on the right and moving left in the product (so 1 is fixed), $2 \mapsto 1 \mapsto 1 \mapsto 3$, next $3 \mapsto 5 \mapsto 5 \mapsto 5$, next $5 \mapsto 2 \mapsto 4 \mapsto 4$, next $4 \mapsto 4 \mapsto 6 \mapsto 6$, and finally $6 \mapsto 6 \mapsto 2 \mapsto 2$ closing the cycle.

We will investigate the structure of S_n in more detail in a bit.

Examples 3. The Dihedral and Quaternion Groups. There are multiple ways to describe these groups, but what we will do here (as a first method) is at the same time illustrate what is meant by generator and relation structure. First the notion of generators.

Definition G4a. We say that a set of elements $\mathcal{S} = \{g_1, g_2, \ldots g_s\} \subseteq G$ is a set of *generators for* G if every element of G can be expressed as a finite product of elements from $\mathcal{S}$ or a inverses from $\mathcal{S}$. We call such a product of elements a *word in* $\mathcal{S}$, in other words G is generated by $\mathcal{S}$ if every element in G is a word in $\mathcal{S}$.

So if $S = \{g_1, g_2, \ldots g_s\}$ then $g_1 g_3^{-1}$ and $g_2^{-1} g_1 g_1 g_1 g_3$ are words in S. (So, the set S is the "alphabet".)

Definition G4b. We say that a word $r_1^{\pm 1} r_2 \cdots r_t^{\pm 1}$ of elements $r_i \in S$ is a *relation* if $r_1^{\pm 1} r_2 \cdots r_t^{\pm 1} = e \in G$.

You can check that $S = \{2, 3, 5, 7, \ldots\} \subset (\mathbb{Q} - \{0\}, \cdot)$ is a set of generators. Then $2 \cdot 3 \cdot 2^{-1} \cdot 5 \cdot 3^{-1} \cdot 5^{-1}$ is a word in S and in fact is a relation.

We next set up a process for constructing groups using generators and relations.

Definition G4c. Abstractly, suppose we have a set S. $\mathcal{R}$ be a set of words in $\mathcal{S}$ which we will call *the relations*. We will say two words in S are equivalent if one can be obtained from the other by canceling inverses and/or multiplying by elements of $\mathcal{R}$ until they coincide. We then say two words are equivalent if they lie in the equivalence class.

For example, for the set of generators $S = \{2, 3, 5, 7, \ldots\} \subset (\mathbb{Q} - \{0\}, \cdot)$. Lets take as relations the set $\mathcal{R} = \{g_1 g_2 g_1^{-1} g_2^{-1} | g_1, g_2 \in S\}$. We then note that $2{\cdot}5{\cdot}7^{-1}$ and $2{\cdot}3{\cdot}5{\cdot}3^{-1}{\cdot}7^{-1}$ are equivalent words. For $2{\cdot}5{\cdot}7^{-1}$ is equivalent to $2 \cdot (3 \cdot 3^{-1}) \cdot 5 \cdot 7^{-1}$ which is equivalent to $2 \cdot (3 \cdot 3^{-1}) \cdot (3 \cdot 5 \cdot 3^{-1} \cdot 5^{-1}) \cdot 5 \cdot 7^{-1}$ which is equivalent to $2 \cdot 3 \cdot (3^{-1} \cdot 3) \cdot 5 \cdot 3^{-1} (\cdot 5^{-1} \cdot 5) \cdot 7^{-1}$ which is equivalent to $2 \cdot 3 \cdot 5 \cdot 3^{-1} \cdot 7^{-1}$. Of course, the set of relations we chose assured that the group generated by S and for which those relations are true is commutative.

Definition G4d. We say that G has a generator-relation structure $(\mathcal{S}, \mathcal{R})$ if
(i)G is generated by $\mathcal{S}$, and
(ii) The elements of G are in one-to-one correspondence with the equivalence classes of words in G generated by the relations $\mathcal{R}$.

Of course the preceding definition is typical of the type of formalizing we do in mathematics where we lay out a fairly simple idea with precision. I put it in this introductory discussion not because I wanted to annoy you at the

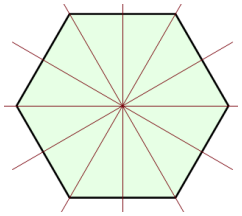
beginning of the course, but because as part of this course you need to learn to read formal definitions and then extract the idea from them that you really need to work with. Basically the definition is saying all elements of G are given as product of elements of $\mathcal{S}$ and their inverses, where we declare relations to be e and cancel them out. One case we will touch on later is the free group on $\mathcal{S}$, which the group with generator-relation structure $(\mathcal{S}, \emptyset)$. As a special case of this we find $\mathbb{Z}$ is the group with generator relation structure $(\{1\}, \emptyset)$. Another simple example is thinking of $\mathbb{Z}/n\mathbb{Z}$ as the group with generator relation structure $(\{1\}, \{1+1+1\cdots+1\})$ where the sum is n 1s.

But for now we will look at the dihedral groups and the quaternion group of order 8.

The Dihedral group D_n. We define D_n to be the group with generator-relation structure $(\{r, s\}, \{r^n, s^2, rsrs\})$. Since the first two relations tell us that $r^{-1} = r^{n-1}$ and $s^{-1} = s$ we can express all elements of D_n as words which are products that are a sequence of alternating r^i and s.

However, the third relation shows that $rs = sr^{-1} = sr^{n-1}$ and so we can keep modifying words by moving all the s entries to the left until every equivalence class of words (e.g. elements of) in D_n is of the from r^i or sr^i where $0 \leq i < n$. In particular we see that D_n has $2n$ elements. Moreover the relations give the following multiplication rules: $(r^i)(r^j) = r^{i+j}$, $(sr^i)(r^j) = sr^{i+j}$, $(r^i)(sr^j) = sr^{j-i}$, and $(sr^i)(sr^j) = r^{j-i}$, where $i + j$ and $j - i$ can be taken (mod n).

We will spend more time with D_n but for now we make a few comments. First, there is the concrete realization of D_n as the group of symmetries of the regular n-gon.



The six symmetries of the hexagon giving D_6

For this you can think of s as being some reflection (doesn't matter which) and r as a rotation of $2\pi/n$ radians. If you haven't seen this, work it out yourself. These are pictured for D_6 in the figure above; the rotations

are represented by the angles through the vertices, while the lines of the reflections pass through the midpoints of the sides.

When $n = 2$ we don't have any regular 2-gons, so in this case we get the abelian group with four elements generated by r, s with $r^2 = s^2 = e$ and $rs = sr$. This is also called the Klein 4-group. It is the unique non-cyclic group of order 4.

The Quaternion group of order eight Q_8. We can also use generators and relations to define a group of order 8, the Quaternion group, which we will denote as Q_8. It can be generated by two elements $\{i, j\}$ but it is customary to list four generators as $\{-1, i, j, k\}$ with relations $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$. Here I am being more informal as my relations are not listed as products giving the identity, but instead listing the relations as we want to use them. (If you are familiar with the division algebra the real quaternions $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ and then you will recognize Q_8 as the multiplicative subgroup of $\mathbb{H} - \{0\}$ generated by i and j.) With the given relations (which are not intended to be a minimal set) one sees that the eight elements of Q_8 are $\{\pm 1, \pm i, \pm j, \pm k\}$.

As an exercise you can check (by verifying the generator-relation structure) the Q_8 is isomorphic to the subgroup of $GL_2(\mathbb{C})$ generated by the matrices $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. More on matrix representations shortly. For now you have met Q_8, one of five possible groups of order 8.

Remark. I close with a remark about multiplication tables. In some introductory texts there are number of pages of multiplication tables for groups. I deliberately don't do that. My reason is that I want you to build mental images of group structure. These structures typically include subgroups of special types where you have developed a solid mental image of the subgroup and if applicable some of the key elements of these subgroups. For example, in the case of the Quaternion group, you want to think about the three subgroups isomorphic to $\mathbb{Z}/4\mathbb{Z}$ generated by i, j, and k. They have the same common element of order 2, namely -1, and then the elements i, j, and k all "anti-commute" in a way that glues together in a way that forms a group with eight elements. This mental image is more useful than staring at a multiplication table, where for sure you will spot these patterns, but I think it is better to hold these ideas in your head as you use the group. As an exercise, if you like, you can certainly write out the multiplication tables for the groups we have discussed.