BMC - Advanced: "Groupdocu" - puzzles with groups

210126 - Chris Overton (handout after lecture 1 on 210120)

This handout summarizes topics we covered last week, as well as recommended reading & problems to prepare for tomorrow's second lecture.

Spoiler alerts: After several questions (often marked **Problem**), there are answers, prefixed by --> . Suggestion: try to think about the problem before looking at the answer.

Caution: this is neither a complete set of notes, nor is it meant as a sole source to introduce these topics - for that, it's best if you also participate in class!

Recently, I covered groups as background material for recent math circles in algebraic topology. Two influences:
1) This reminded me how cool groups are on their own
2) As I was working out a group multiplication table, a comment by Ted Alper (Stanford pre-collegiate studies): "this is like Sudoku"**(to be explained shortly...)

Hence, we're presenting this as a series of puzzles!

Getting to know groups (Topics for the first day):

- groups: definitions & properties
- understand what we take for granted (commutativity, associativity) and changing habits when we can't
- we throw lots of definitions and tricks at you, and illustrate how they fit together!
- useful concepts: conjugacy, actions, subgroups, normal subgroups, centers, ..
- useful machinery for contructing groups and working with them: presentations, permutations, sylow theorems
- experience working out lots of examples

Plan for second day: additional experience with several special examples, more thoerems

- more on conjugacy and commutators: measuring how much groups and elements fail to be abelian
- every finite group can be thought of as a permutation group. How can we use this?
- every finite group can be described using generators and relations
- "multiplying" and "dividing" by groups - how "normal" subgroups are special => that means a way to understand all groups is to see how they can be extended from "simple" groups (those without nontrivial normal subgroups.)
- the structure of finite abelian groups
- working out more examples, especially p-groups
- hopefully build confidence in you as an aspiring group theorist (as opposed to group therapist)

Definition: a group G is a set of elements $\{g_i \dots\}$ and an **operation** $*$ (here called "multiplication/times") so that:

- The operation is defined: $\forall g_1, g_2 \in G : g_1 * g_2 \in G$
- **Associative**: $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$
- There is a **neutral element** (often written as **1**) such $1 * g = g * 1 = g$
- For any g there is an **inverse element** g^{-1} such that $g^{-1} * g = g * g^{-1} = 1$

Caution! We did not say the operation is commutative (= "**abelian**"), which would mean always $g_1 * g_2 = g_2 * g_1$ (g_1 "commutes" with g_2.) You have to change your habit of assuming this, and realize how to work differently with non-abelian groups!

Remember, some elements can commute even in non-abelian groups.

If a group is abelian, the operation is sometimes written as "+", the neutral element as "0", and inverses as "-g".

Let's work out our first examples (try to answer each question before peeking at the answer!)

- Are there any groups with **no** elements?

--> No, this has no "neutral" element.

- Are there any groups with **one** element?

--> Yes, the "trivial" group than has only the element 1.

- How many groups are there with **two** elements (i.e. of "**order**" two)?

--> There's exactly one such group. Give the name "a" to the element other than 1. Then there is no other element that could be the inverse of a, which works out the entire multiplication table. So even though we could name the group and its elements differently, we say there is only 1 group of order 2 (up to isomorphism.)

Definition: the **order** of a group G (written $|G|$) is its number of elements; the order of an element $g \in G$, written $|g|$, is the lowest n for which $g^n = 1$, namely how many times you have to multiply it by itself to get to the neutral element (could be ∞)

Introducing multiplication tables ("Cayley tables")

A group can be specified by its multiplication table. Here is one for a group of order 4 called the "Klein group":

	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

The row and column headers (respectively in column zero and row zero) tell you what you are multiplying. For example, the item in position (2, 3) is in the row for a and the column for b, and tells you that $a * b = ab$, meaning you get the element called "ab".

A multiplication table need not form a group. You also need a neutral element (here in row 1 and column 1), each element has to have an inverse (so the neutral element has to appear as a result in each row and each column), **and** the operation has to be associative (more on that later!)

By convention, we will always put the neutral element in the first row and in the first column. In this case, the row headers are equal to elements in the first row of answers, e.g. because $a * 1 = a$. Similarly for columns. So we can make our tables smaller by just leaving out the headers and reading them from first row and first column. Written this way, the multiplication table above looks like:

1	a	b	ab
a	1	ab	b
b	ab	1	a
ab	b	a	1

By the way: note that the first two elements by themselves also form a group. When a subset of a group forms its own group, it is called a subgroup, written $H \leq G$. Can you find any other subgroups?

You can check that this group is **abelian** (=**commutative**): when multiplying two elements, you get the same product whichever one you put first. One way to see this is because the multiplication table is symmetric about the diagonal axis. (In this case, it consists only of 1's, but that is not needed for commutativity.)

You will have to break the habit of assuming commutativity! [Example shown in class: rotations of an object around different axes can be shown not to commute.]

Side note on associativity

For a group of order n, there are n^2 products in the multiplication table. To check associativity, you would have to check n^3 equations - this starts to become a nuisance!

Just to show you can't ignore this, here is a multiplication table of "**octonians**." These are not associative.

Here each e_i is a separate dimension over the real numbers. But we can also think of this as just 16 different elements $+/-e_i$, with e_0 the neutral element. Here "-" commutes with everything, so we use an 8 by 8 table as a shortcut for a 16 by 16 table.

Problem:
a) Show each element has an inverse
b) Show this is not a group, because multiplication is not associative

$e_i e_j$		e_j							
		e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_i	e_0	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
	e_1	e_1	$-e_0$	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
	e_2	e_2	$-e_3$	$-e_0$	e_1	e_6	e_7	$-e_4$	$-e_5$
	e_3	e_3	e_2	$-e_1$	$-e_0$	e_7	$-e_6$	e_5	$-e_4$
	e_4	e_4	$-e_5$	$-e_6$	$-e_7$	$-e_0$	e_1	e_2	e_3
	e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	$-e_0$	$-e_3$	e_2
	e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	$-e_0$	$-e_1$
	e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	$-e_0$

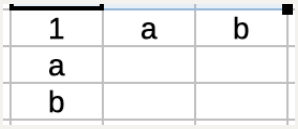
--> a) For example, the table shows $e_2 * e_2 = -e_0$, which means $e_2 * -e_2 = e_0$, the neutral element. So $e_2^{-1} = -e_2$, or the inverse of e_2 is $-e_2$. More generally, you can find an inverse to each element, because there is always e_0 or $-e_0$ in each row (or column.)
Specifically, e_0 and $-e_0$ are each their own inverse, and for $i \neq 0$, $e_i^{-1} = -e_i$, $(-e_i)^{-1} = e_i$.

--> b) Sometimes, this multiplication is associative, so you have to hunt around for a case when it isn't. For example: $(e_1 * e_2) * e_4 = e_3 * e_4 = e_7 \neq -e_7 = e_1 * e_6 = e_1 * (e_2 * e_4)$

In general, it would take a lot of work to show associativity if we have to verify it for all n^3 lists of 3 elements of G. But in the cases we consider, we usually don't write multiplication tables completely from scratch, but instead consider generators and relations, in which case groups "inherit" associativity as **quotients** of **free groups**. Similarly, permutations are inherently associative, and so are groups defined as permutations.

- How many groups are there with **three** elements?

--> Here it helps to work out a multiplication table. Call the elements 1, a, and b. It is easy to start filling out the table:



1	a	b
a		
b		

But what is $a * a$? At this point, it may seem that it would be either 1, a, or b, but the following mini-theorem makes our work easier:

The Groupdocu theorem: each row (resp. column) of a group G's multiplication table is a permutation of the group's elements - i.e. it contains each element of G exactly once.

Proof For example, labeling the elements of G by indexes, suppose the value g_k occurs twice in row i, namely in columns j_1 and j_2. Then we would have:
$g_i * g_{j_1} = g_k = g_i * g_{j_2}$

We can multiply this equation **on the left** by g_i^{-1} to obtain (left and right ends):
$g_i^{-1} * (g_i * g_{j_1}) = g_i^{-1} * (g_i * g_{j_2})$

Now we use the associative rule on each end, and in both cases the first factor is $g_i^{-1} * g_i = 1$, which cancels out, leaving $g_{j_1} = g_{j_2}$.

As you learn group theory (and algebra, for that matter) you'll see and do lots of proofs with this kind of logic!

Getting back to the multiplication table above, $a * a$ is thus either 1 or b, since a is already taken in a's row. But if $a * a = 1$, then the only element left to fill in for $a * b$ would be b. But you can't have $a * b = b$, because you already have $1 * b = b$ and two values b in b's column would violate the Groupdocu theorem!
So $a * a = b$, and it is easy to fill out the table from there - showing there is exactly one group of order 3.

By the way, once we know this, we can just call the element b by the name of a^2, and now everything is defined in terms of one generator a, and it follows this multiplication is associative. The table is shown as G (on the left):

G, with operation *			→	H, with operation +		
1	a	a^2		0	1	2
a	a^2	1		1	2	0
a^2	1	a		2	0	1

But there is another way we can think of the table (shown as H on the right.)
H uses the operation of addition (+), and now the table for the operation is an addition table, not a multiplication table. H's operation is associative for the same reason, and its neutral element is 0.
The way we can see the two groups are "the same" is to note there is a map between elements (call it "f") that maps row headers as shown (e.g. $f(a) = 1$.)
We can see that this map also "respects" the two operations, for example as follows:
$f(a * a^2) = f(1) = 0 = 1 + 2 = f(a) + f(a^2)$

In other words, f turns "*" into "+", and "commutes" with the two different operations of groups G and H. Such a map is called a **homomorphism** (more generally, just **morphism**).

There are several more specific kinds of morphisms:

- An **isomorphism** can be done backwards, as for example for f.
- An **epimorphism** maps **onto** each element of its target group, again as is true for f. But f would no longer be an epimorphism if H also contained other elements that are not images $f(g_i)$ for any g_i.
- A **monomorphism** maps **1-1**, meaning two different elements never have the

same image. A counterexample would be the map "**0**" (which we think of as a function, not an element!) that maps all of G to the element 0 in H.
This is in fact a homomorphism (a trivial one), but it is not a monomorphism, nor is it an epimorphism.

As the order increases, there are more possible groups:

- How many different groups are there with four elements?

--> We showed the two groups in class. Using the "groupdocu theorem", you can work out that you get the table above ("Klein group") if no element has order 4, in which case, the only possible order of elements is 2. If you do have elements of order 4, call one of them a, and you can see that a good way to define this is just as a group generated by one element a, such that $a^4 = 1$. Here we write this as a **presentation**, first listing one generator, and then showing the **relation** satisfied the the generator:
$\mathbb{Z}/4 =< a|a^4 = 1 >$
Such a group is called "cyclic"

Note: this suggests thinking of the group in two isomorphic ways: the notation $\mathbb{Z}/4$ stands for taking the integers $\mathbb{Z}$ (with operation addition), and "dividing" them by 4, or really by the sugbroup $4 * \mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, \dots\}$

- How may groups are there with five elements?

--> By now, you should be getting used to the idea that for any positive n, there is a cyclic group of order n generated by 1 element a: $\mathbb{Z}/n =< a|a^n = 1 >$

But is this the only possibility for five elements? if we try to write out a multiplication table, starting with a^2, the groupdocu rule is less helpful.

So we ask how big is the subgroup H generated by a? This turns out to be a very helpful result, whose proof uses the important technique of cosets.

Definition, for a subset $H \subset G$, and an element $g \in G$, the (right) **coset** is defined as $Hg = \{h * g \text{ for } h \in H\}$. Similarly, one can define left cosets gH.

Lemma: If $H \leq G$, the cosets $\{Hg_i \text{ for } g_i \in G\}$ partition all the elements of g - i.e. each element $g \in G$ is in exactly one coset, represented by one of the g_i.

Proof: try to prove this on your own, and we'll review it in class!

The number of cosets for H in G is written $[G : H]$.

Lagrange's theorem: for a subgroup H of a finite group G, the orders divide: $|H| \mid |G|$. Specifically, $|G| = |H|[G : H]$

(Notice how the notation is building up?!)

Proof: each coset has the same number of elements as H ■
(The blacksquare means we're done proving the theorem. Make sure you understand the proof!)

Corollary: the order $|g|$ of $g \in G$ divides $|G|$

Prove this.

Now back to groups of order 5: any element that is not order 1 (namely anything other than the neutral element) has to have order 5, since there are no other orders that could divide 5. Therefore, all groups of order 5 are isomorphic to the cyclic group.

More generally, **all groups of prime order are cyclic.**

- How may groups are there with six elements?

--> There is certainly the cyclic group $\mathbb{Z}/6 =< a|a^6 = 1 >$.

But note that in order 4 we saw hints at another way to make a group: we can take two groups $H = \mathbb{Z}/2 =< a|a^2 = 1 >$ and $K = \mathbb{Z}/2 =< b|b^2 = 1 >$ and take their abelian product ("direct product") $G = H \bigoplus K$ by saying everything in H commutes with everything in K, and specifying elements of G as pairs $\{(h, k)|h \in H, k \in K\}$
Here the set $\{(h, 1)|h \in H\}$ is isomorphic to H, and we think of these as the same thing (similarly for K.)

This is a convenient way to make new groups, and a group specified this way is easy to understand.

Problem What group is $\mathbb{Z}/2 \bigoplus \mathbb{Z}/3$?

--> Homework - we'll discuss in class.

6 is the first order for which there is a non-abelian group S_3: the **permutations** of 3 objects (1, 2, and 3.) We write such permutations in **cycle notation**. For example, (1 2) is the permutation that sends 1->2 and 2->1 (the end of a cycle gets sent back to its beginning.) Also, any element not shown in the cycle gets sent to itself. So another way of showing the same permulation would be (1 2)(3).

We will spend a lot of time with this group, so let's write out its table, including three specially named elements (a, b, and c):

1	(1 2)=a	(1 3)	(2 3)=c	(1 2 3)=b	(1 3 2)
(1 2)=a	1	(1 2 3)	(1 3 2)	(1 3)	(2 3)
(1 3)	(1 2 3)	1	(1 2 3)	(2 3)	(1 2)
(2 3)=c	(1 3 2)	(1 2 3)	1	(1 2)	(1 3)
(1 2 3)=b	(1 3)	(2 3)	(1 2)	(1 3 2)	1
(1 3 2)	(2 3)	(1 2)	(1 3)	1	(1 2 3)

CAUTION: the way we write it, the column header shows which permutation acts **first** and the row header shows what happens next. So $a * b = (12) * (123)$ means:
$1 \to 2 \to 3, 2 \to 1 \to 2, 3 \to 3 \to 1$
In each list, the first arrow is the action of (1 2), and the second arrow that of (1 2 3).
You can think of the permutations sitting on the right side of what they permute, and to multiply, you go from right to left. This is called "acting on the right."

By contrast, functions are often though to "act on the left", so given functions f and g, their product $f \circ g$ is typically defined as $(f \circ g)(x) = f(g(x))$, so "g happens first." Now that we are in a nonabelian world, you have to sweat these details!

Problem (to be reviewed in class) Consider these two subgroups generated by single elements: $H =< (12) >$ and $K =< (123) >$

- What are their orders?
- What are left cosets of H in G? What about the right cosets?
- What are the left cosets of K in G? What about the right cosets?
- Is $S_3 = H \bigoplus K$?

Normal subgroups

If $M \leq G$, if for any $g \in G$, $g^{-1}Mg = M$, we say M is **normal** in G, written $M \trianglelefteq G$ (note the different sign with a triangle instead of just <.)

Normal groups let you do all kinds of cool things like taking a quotient G/M, as we'll discuss more.

For now:

Problem: Is $H \trianglelefteq S_3$? Is $K \trianglelefteq S_3$?

Problem: what are all the normal subgroups of $\mathbb{Z}/5$? What about of the Klein group?

--> Hint both the trivial group <1> and entire group are normal in itself. If a group has no other normal subgroups, it is called **simple**. See if you can find any other normal subgroups besides these "trivial" ones.

Other topics we'll mention tomorrow:

The structure of finite abelian groups

These are easy, partly because every subgroup of an abelian group is normal.

Conjugation and conjugacy classes

A **conjugate** of g by h is $h^g = g^{-1} * h * g$. If h commuted with g, you would have simply $h^g = h$, so conjugation moves things around only when, and to the extent that, they don't commute. You can define a similar conjugate of a whole set of elements, like of a subgroup.

Problem what are the conjugates of (1 2) in S_3? How does this relate to the question: what are the conjugates of $H = (12)$ in S_3?

To give you a sense of how ueful this is:

Definition: a **p-group** for a prime p is a group whose order is p^n for positive integer n.

Definition: the **center** $Z(G)$ of a group G is the set of elements that commute with everything: $\{c \in G | c * g = g * c, \forall g \in G\}$.

Theorem: Every p-group has a center consisting of more than just the neutral element.

Corollary: Prove that there are only two groups of order p^2 for p prime - just the abelian groups $\mathbb{Z}/p^2$ and $\mathbb{Z}/p \bigoplus \mathbb{Z}/p$

Sylow theorem: if p^k is the highest power of p that divides the order $|G|$ of G:

- G has subgroups of order p^k
- The number of these is $\equiv 1$ (mod p)
- They are all conjugate in G

Every group is a permutation group

Prove this

--> Hint, you can think of how each element g permutes the set of elements on G by multiplying on the right side...

But, you might also be able to think in terms of cosets.

Problem Using all you have learned so far, how many groups are there of order 8? First, how many abelian groups?

Non-abelian finite groups can get very complicated! No one has found a clean way to classify them, even though one of the big 20th century triumphs of math was to classify all the finite simple groups.

Motivating thought, from "The Theory of p-Groups", by David A. Craven, '08:

In the table below, $g(n)$ is the number of groups of order n. What patterns do you notice?

n	$g(n)$	n	$g(n)$	n	$g(n)$	n	$g(n)$
1	1	11	1	21	2	31	1
2	1	12	5	22	2	32	51
3	1	13	1	23	1	33	1
4	2	14	2	24	15	34	2
5	1	15	1	25	2	35	1
6	2	16	14	26	2	36	14
7	1	17	1	27	5	37	1
8	5	18	5	28	4	38	2
9	2	19	1	29	1	39	2
10	2	20	5	30	4	40	14

Conclusion

You have now been exposed to many of the concepts in a standard undergrad course in group theory. After next time, you will have more experience with standard results.

But you already have enough tools to work out lots of examples.
Suggested effort: try to work out all the different groups of orders up to 15!

If you want a bigger challenge, try the groups of order 16.

Recommended sources:

One very clear and succinct exposition is: "Notes on finite group theory" by Peter J. Cameron (13) - available online.

Here is a good recent undergrad text, but it's still easy to get lost in all the many definitions and theorems: