**Homework #3 – Key**

HW due Sunday 2/9 by pdf upload to Canvas; .tex source on the MATH 312 github repo.

## Stuff about permutation groups and $S_n$

**Problem 1.** (Omitted from key bc any reasonable explanation is correct.)

**Problem 2.** Suppose that $g, h \in G$. We mentioned in class that the *conjugate* of $h$ by $g$ is the element $ghg^{-1}$. The *conjugacy class* of $h$ is the set of all the possible conjugates of $h$: $\{ghg^{-1} \mid g \in G\}$.

- Find the conjugacy classes of all six elements of $S_3$. (If you use the permutation calculator, make sure you're multiplying left-to-right!)
  - Identity: $\{e\}$
  - Transpositions: $\{(1\ 2), (1\ 3), (2\ 3)\}$
  - 3-cycles: $\{(1\ 2\ 3), (1\ 3\ 2)\}$
- If you are having fun, find the conjugacy classes of all 24 elements of $S_4$.
  - Identity: $\{e\}$
  - Transpositions: $\{(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)\}$
  - Double transpositions: $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$
  - 3-cycles: $\{(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}$
  - 4-cycles: $\{(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\}$

**Problem 3.** Suppose $\sigma \in S_n$, and that $|\sigma| = k$.
Please note that I am writing out the details of this proof very carefully, so that it is clear at each step what is my data and what is my claim. As is usual, most of the warrants are "implicit;" see if you can fill in the warrants that connect the data to the claims.

- Explain why $\sigma^k$ is an even permutation.

  Since $|\sigma| = k$, $\sigma^k = e$. The identity permutation $e$ is an even permutation, as it takes 0 transpositions to write. Therefore, $\sigma^k$ is an even permutation.

- Suppose that $\sigma$ is an odd permutation. Is $k$ even or odd? How do you know?

  Let $t$ be the number of transpositions it takes to write $\sigma$. Since $\sigma$ is an odd permutation, we know that $t$ is an odd number.

  Now consider $\sigma^k = \underbrace{\sigma \cdot \sigma \cdot \ldots \cdot \sigma}_{k \text{ times}}$. How many total transpositions is that? Since each copy of $\sigma$ represents $t$ transpositions, $\sigma^k$ represents $t \cdot k$ total transpositions.

  But $\sigma^k = e$ is an even transposition, so $t \cdot k$ must be an even number. Therefore, since $t$ is odd, $k$ must be even.

- Conclude that a cycle of odd length is an even permutation. Feel moderate annoyance.

  The order of a cycle is the same as its length. For instance, the order of a transposition like (1 3) is 2; the order of a 3-cycle like (1 2 3) is 3.

  Suppose $\sigma$ is a cycle of odd length. Therefore its order must also be odd. So, if $|\sigma| = k$, then $k$ is an odd number.

  Again, let $t$ be the number of transpositions it takes to write $\sigma$. Again, $\sigma^k$ requires $t \cdot k$ transpositions to write. Since $\sigma^k = e$, which is an even permutation, we know that $t \cdot k$ must be an even number.

  Now, since $t \cdot k$ is an even number but $k$ is an odd number, we conclude that $t$ is an even number. Therefore $\sigma$ is an even permutation, by the definition of even permutations.

**Problem 4.** Play a bit more with Cayley's theorem:

- Extract from the Cayley diagram of $C_4 \times C_2 = \langle r, b \rangle$ the two permutations that describe its arrows, and therefore describe $C_4 \times C_2$ as a subgroup of a symmetric group.

  A key step in this process is to relabel the nodes with the numbers 1-8 (in this case; if the group had order 12 then it'd be the numbers 1-12, etc.). It doesn't really matter how you choose to number the nodes, but you do have to number them. To make my point, I've chosen labels for both $C_4 \times C_2$ and $Q_8$ that I don't think anybody else would have used.

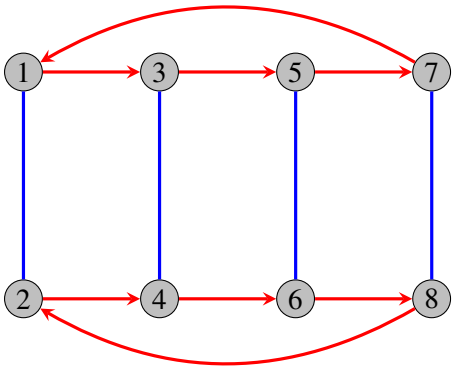
  With the number labels I've assigned in the diagram below,

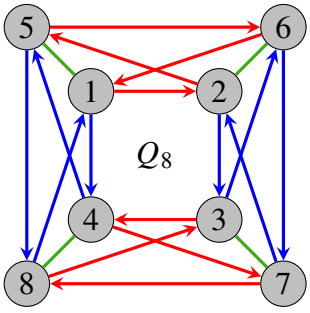
$$C_4 \times C_2 \cong \langle (1\ 3\ 5\ 7)(2\ 4\ 6\ 8), (1\ 2)(3\ 4)(5\ 6)(7\ 8) \rangle.$$

- Do the same for $Q_8 = \langle i, j, -1 \rangle$.

  With the number labels I've assigned in the diagram below,

$$Q_8 \cong \langle (1\ 2\ 5\ 6)(3\ 4\ 7\ 8), (1\ 4\ 5\ 8)(2\ 3\ 6\ 7), (1\ 5)(2\ 6)(3\ 7)(4\ 8) \rangle.$$




## Stuff about direct products

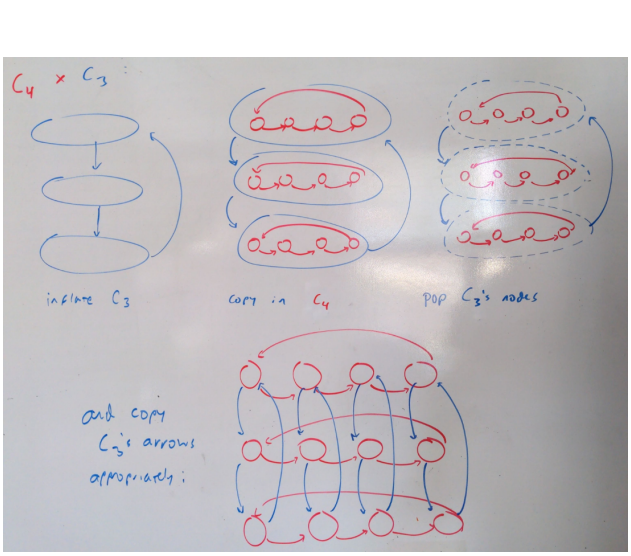
**Problem 5.** I want to make the relationship between the inflate-the-Cayley-diagram description and the ordered-pairs description of a direct product a bit more evident. Say that $C_4 = \langle r \mid r^4 = 1 \rangle$ and $C_3 = \langle b \mid b^3 = 1 \rangle$.

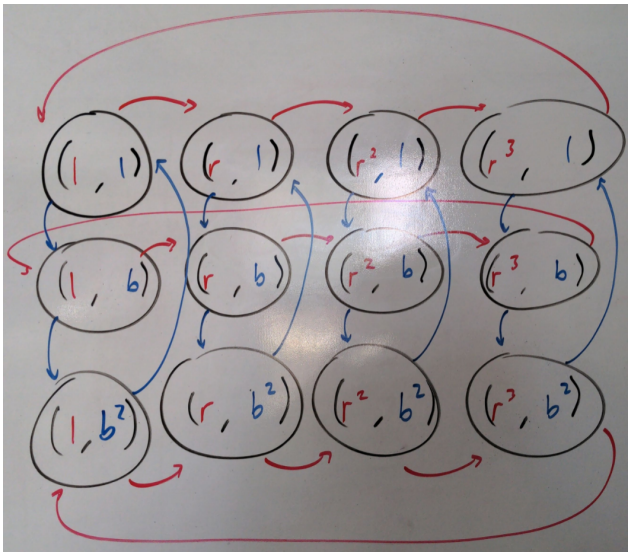
- Write out all 12 elements of $C_4 \times C_3$ as ordered pairs. (They will all look like $(r^k, b^j)$.)

$$\begin{array}{cccc} (1,1) & (r,1) & (r^2,1) & (r^3,1) \\ (1,b) & (r,b) & (r^2,b) & (r^3,b) \\ (1,b^2) & (r,b^2) & (r^2,b^2) & (r^3,b^2) \end{array}$$

- Use the inflation procedure to draw the Cayley diagram of $C_4 \times C_3$.
- Label each node in your Cayley diagram with the corresponding ordered pair.

  I am emphasizing that it is 100% fine to draw your diagram by hand. It took me, and I timed it, 14 minutes to draw these two diagrams, and that includes going upstairs to get new markers. I promise it would have taken me way longer than that to do this in tikz.



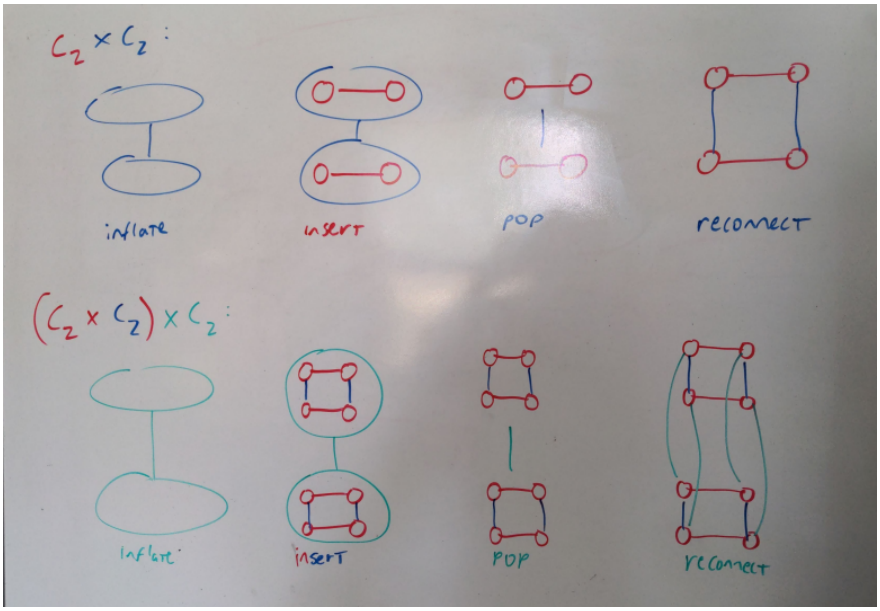



- (Bonus problem: Is $C_4 \times C_3$ "secretly cyclic"?) ''(Yes, it is generated by $(r, b)$!)

**Problem 6.** Explore $C_2 \times C_2 \times C_2$.

- Figure out how to repeat the inflation process to draw a Cayley diagram.

  Can you tell that I was thinking of this as $(C_2 \times C_2) \times C_2$? How do you think I would have drawn this a bit differently if I was thinking of it as $C_2 \times (C_2 \times C_2)$?

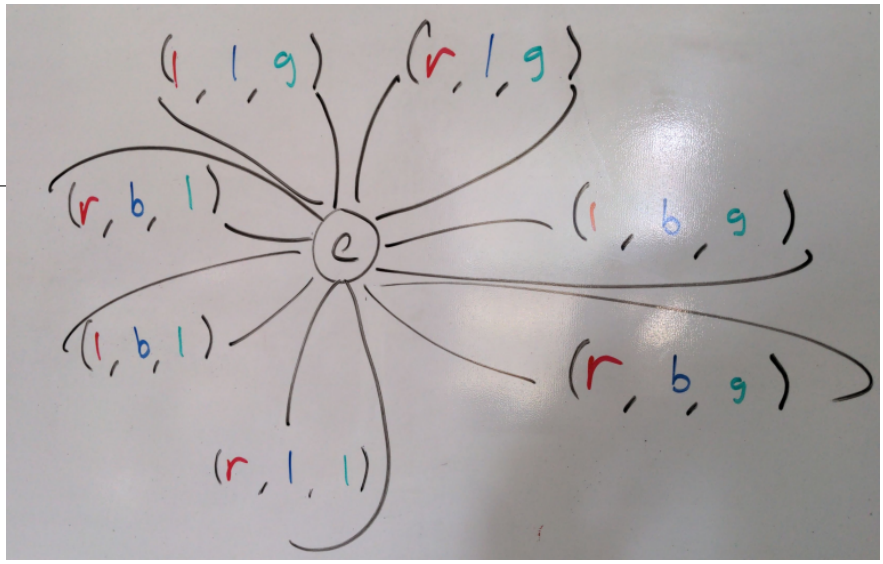



- Compute the orbits of each of the 8 elements and draw a cycle graph.

  I am thinking of $C_2 = \langle r \rangle$, $C_2 = \langle b \rangle$, and $C_2 = \langle g \rangle$.

  Challenge: think about $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, written additively.

| Element | Orbit |
|---|---|
| $(1,1,1) = e$ | $\{e\}$ |
| $(r,1,1)$ | $\{e, (r,1,1)\}$ |
| $(1,b,1)$ | $\{e, (1,b,1)\}$ |
| $(r,b,1)$ | $\{e, (r,b,1)\}$ |
| $(1,1,g)$ | $\{e, (1,1,g)\}$ |
| $(r,1,g)$ | $\{e, (r,1,g)\}$ |
| $(1,b,g)$ | $\{e, (1,b,g)\}$ |
| $(r,b,g)$ | $\{e, (r,b,g)\}$ |




- Is this a new group? Groups of order 8 we already know are $C_8$, $C_4 \times C_2$, $D_4$, and $Q_8$.

  This is definitely a new group, because everybody in this group has order 2 (as is easy to see in the cycle graph), but that's not true of any of the other groups of order 8 we know!

**Problem 7.** Prove using algebra that $A \times B$ is abelian if and only if both $A$ and $B$ are abelian.
*Hint:* Remember that an "if and only if" statement is actually looking for *two* proofs.
Same note as previously: Please note that I am writing out the details of this proof very carefully, so that it is clear at each step what is my data and what is my claim. As is usual, most of the warrants are "implicit;" see if you can fill in the warrants that connect the data to the claims.

($\Rightarrow$) Suppose that $A$ and $B$ are both abelian.
Let $a, x \in A$ and $b, y \in B$.
Since $A$ and $B$ are abelian,

$$ax = xa \text{ and } by = yb.$$

Consider $(a, b), (x, y) \in A \times B$.

$$\begin{aligned}(a, b) \cdot (x, y) &= (ax, by) \\ &= (xa, yb) \\ &= (x, y) \cdot (a, b).\end{aligned}$$

Therefore, $A \times B$ is abelian.

($\Leftarrow$) Suppose that $A \times B$ is abelian.
Let $(a, b), (x, y) \in A \times B$.
Since $A \times B$ is abelian,

$$(a, b) \cdot (x, y) = (x, y) \cdot (a, b).$$

But then $(ax, by) = (xa, yb)$,
so $ax = xa$,
and $by = yb$.
Therefore, $A$ and $B$ are both abelian.

**Problem 8.** Here we'll explore when the product of cyclic groups is "secretly cyclic".
Same note as previously: Please note that I am writing out the details of this proof very carefully, so that it is clear at each step what is my data and what is my claim. As is usual, most of the warrants are "implicit;" see if you can fill in the warrants that connect the data to the claims.

(a) Say you have a generic group $G$ such that $|G| = n$. Suppose further that you found an element $g \in G$ such that $|g| = n$. Prove that $G$ is cyclic. (Hint: look at the orbit of $g$, and think about the definition of $|g|$.)

Since $|g| = n$, we know $g^n = e$ and $g^k \neq e$ for any $k < n$. Therefore, the orbit of $g$ is $\langle g \rangle = \{g, g^2, \ldots, g^{n-1}, g^n = e\}$, and all those powers of $g$ are distinct.

(How do we know all those powers are distinct? If $g^a = g^b$ for some $a, b < n$, then $g^{b-a} = e$ with $b - a < n$, but that contradicts the fact that $|g| = n$.)

$g^k \in G$ for every $k \in \mathbb{Z}$, so this list of $n$ distinct elements must be precisely all of $G$.

Therefore, $G = \langle g \rangle$, so $G$ is cyclic.

(b) Suppose that $a, b \in \mathbb{Z}$ are relatively prime. (Google it if you don't remember what this means.) Fact: $\text{lcm}(a, b) = ab$. Optional challenge: prove it.

This proof is actually somewhat involved! You have to know the "Euclidean algorithm" aka integer division with remainder. That's why it was optional. :)

(c) Consider the direct product $\mathbb{Z}_a \times \mathbb{Z}_b$, with $a$ and $b$ relatively prime. What is $|(1, 1)|$?

(**NOTE TYPO FIX:** I had previously written $C_a \times C_b$, in which the element $(1, 1)$ would represent the identity. I could also have said, suppose that $C_a = \langle g \rangle$ and $C_b = \langle h \rangle$ and then think about the element $(g, h) \in C_a \times C_b$, but I think it's cleaner this way.)

Okay so here's the deal. The main reason I wanted to write this key was to resolve the issue with the typo here. I am going to write this proof two ways: first with the groups **written additively**, as suggested here, and then **written multiplicatively**.

**Written additively**: $\mathbb{Z}_a$ and $\mathbb{Z}_b$ are both generated by repeatedly adding the element 1, but in $\mathbb{Z}_a$, $|1| = a$, and in $\mathbb{Z}_b$, $|1| = b$. To help us distinguish between these two different versions of 1, I'm going to write $\mathbb{Z}_a = \langle 1_a \rangle$ and $\mathbb{Z}_b = \langle 1_b \rangle$; note in particular that $1_a \cdot a = 0$ and $1_b \cdot b = 0$ (because 0 is the identity element here).

Consider the element $(1_a, 1_b) \in \mathbb{Z}_a \times \mathbb{Z}_b$. I claim that $|(1_a, 1_b)| = \text{lcm}(a, b)$. By the definition of order, $|(1_a, 1_b)|$ is the smallest $k$ such that $(1_a \cdot k, 1_b \cdot k) = (0, 0)$. But looking in the $\mathbb{Z}_a$ component, this means that $k$ is a multiple of $a$, and looking in the $\mathbb{Z}_b$ component, this means that $k$ is a multiple of $b$. Therefore, $k$ is a common multiple of $a$ and $b$, and since $k$ is the *least* such number, $k = \text{lcm}(a, b)$.

Since $a$ and $b$ are relatively prime, $\text{lcm}(a, b) = ab$, so $k = ab$, so $|(1_a, 1_b)| = ab$.

**Written multiplicatively**: Very similar. I literally am copy-pasting and modifying.

$C_a = \langle g \rangle$ and $C_b = \langle h \rangle$ are both generated by repeatedly multiplying their generating element. In $C_a$, $|g| = a$, and in $C_b$, $|h| = b$. Note in particular that $g^a = e$ and $h^b = e$ because $e$ is the name of the identity element here.

Consider the element $(g, h) \in C_a \times C_b$. I claim that $|(g, h)| = \text{lcm}(a, b)$. By the definition of order, $|(g, h)|$ is the smallest $k$ such that $(g^k, h^k) = (e, e)$. But looking in the $C_a$ component, this means that $k$ is a multiple of $a$, and looking in the $C_b$ component, this means that $k$ is a multiple of $b$. Therefore, $k$ is a common multiple of $a$ and $b$, and since $k$ is the *least* such number, $k = \text{lcm}(a, b)$.

Since $a$ and $b$ are relatively prime, $\text{lcm}(a, b) = ab$, so $k = ab$, so $|(g, h)| = ab$.

(d) Conclude that $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{ab}$.

Finally, we can apply the result of part (a) to conclude that since $|\mathbb{Z}_a \times \mathbb{Z}_b| = ab$, and since $|(1_a, 1_b)| = ab$, $\mathbb{Z}_a \times \mathbb{Z}_b$ is cyclic, generated by $(1_a, 1_b)$. Therefore, $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{ab}$, the (additive) cyclic group of order $ab$.

Finally, we can apply the result of part (a) to conclude that since $|C_a \times C_b| = ab$, and since $|(g, h)| = ab$, $C_a \times C_b$ is cyclic, generated by $(g, h)$. Therefore, $C_a \times C_b \cong C_{ab}$, the (multiplicative) cyclic group of order $ab$.