

Math Circles - Group Theory, Selected Solutions

Tyrone Ghaswala - ty.ghaswala@gmail.com

4th, 11th, 18th February 2015

Here are solutions to some of the questions. Not all solutions appear here for two reasons. First, a whole bunch of the questions are answered (at least partially) somewhere in the notes, usually after the question has been posed. Second, I don't want to ruin the fun for you by giving you all the answers!

Question Sheet 1

2. We exclude 0 because it doesn't have a multiplicative inverse. As we'll see later, every element in a group must have an inverse.

3. (a) The table is

\times	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(b) The identity in this group is the element 1.

(c) The inverses for each element are give in the following table.

x	1	-1	i	$-i$
x^{-1}	1	-1	$-i$	i

5. The elements of \mathbb{Z}_8^* are $\{1, 3, 5, 7\}$ and the multiplication table is given by

\times	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

The order of the group is $|\mathbb{Z}_8^*| = 4$.

6. The orders of the groups are given as follows.

G	\mathbb{Z}_n	\mathbb{Z}_p^*	Poly(n)	Sym(n)	Braid(3)	\mathbb{Z}
$ G $	n	$p-1$	$2n$	$n!$	∞	∞

9. The Rubik's cube is a group where each element is a move (say rotate the top layer by 90 degrees), and the operation is composition, that is do one move and then the other. A bit of thought will convince you that this is indeed a group, where the identity is the "do nothing" move.

Question Sheet 2

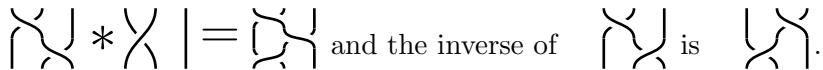
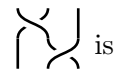

1. (b) The groups \mathbb{Z}_6 and $\mathbb{Z}_2 \times \mathbb{Z}_3$ are isomorphic, and the groups $\text{Poly}(3)$ and $\text{Sym}(3)$ are isomorphic. However, \mathbb{Z}_6 is not isomorphic to $\text{Poly}(3)$ and one way to see this is that in \mathbb{Z}_6 , $a + b = b + a$ for all elements. However in $\text{Poly}(3)$, $a * b \neq b * a$ for all $a, b \in \text{Poly}(3)$.
2. Up to isomorphism, there are two groups of order four, isomorphic to $(\mathbb{Z}_4, +)$ and (\mathbb{Z}_2^*, \times) . There is only one group of order 5. In fact, it follows from Lagrange's theorem (which comes at the end of the course) and a bit of work, that there is only one group of order p for any prime, and it is isomorphic to $(\mathbb{Z}_p, +)$.
3. The copy of $(\mathbb{Z}_3, +)$ is given by the subset $\{e, r_1, r_2\}$ in $\text{Poly}(3)$. We can see this copy if we replace e with 0, r_1 with 1, and r_2 with 2. This actually gives us an isomorphism between \mathbb{Z}_3 and $\{e, r_1, r_2\}$. You can see the copy of $\text{Poly}(n)$ in $\text{Sym}(n)$ by labelling the corners of the n -gon, and labelling the dots in $\text{Sym}(n)$. Then for each element of $\text{Poly}(n)$, you can find it in $\text{Sym}(n)$ by keeping track of how the element of $\text{Poly}(n)$ permutes the corners, and doing the same in $\text{Sym}(n)$.

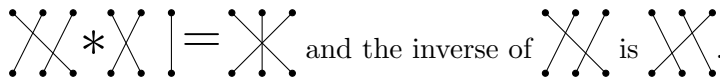
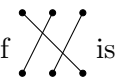

The notion of finding a copy of another group in a bigger group leads to the definition of subgroups in the notes.

4. The orders of elements $x \in \mathcal{Q}_8$ are given as follows.

$$\begin{array}{c|c|c|c|c|c|c|c|c|c} x & 1 & -1 & i & -i & j & -j & k & -k \\ \hline |x| & 1 & 2 & 4 & 4 & 4 & 4 & 4 & 4 \end{array}$$

5. *Proof.* Suppose $ba = e = ca$, then $ba = ca$. Multiplying on the right by a^{-1} we get $b = c$, and so inverses are unique. ■
6. *Proof.* Suppose we have two elements e, f such that $ea = a = fa$. Then $ea = fa$ and multiplying on the right by a^{-1} we have $e = f$ so identities are unique. ■

8. (a) i.  and the inverse of  is .

- ii.  and the inverse of  is .

- (b) i. $6 + 7 = 13$ and the inverse of 8 is -8 .
ii. $6 + 7 = 4$ and the inverse of 8 is 1.

9. \mathbb{Z}_4 and $\{1, -1, i, -i\}$ have generators (1 and i respectively), but \mathbb{Z}_8^* does not. Given two groups of the same order with generators, we can find an isomorphism by simply replacing one generator and all its powers with the other generator. From this we can conclude that \mathbb{Z}_4 is isomorphic to $\{1, -1, i, -i\}$ but \mathbb{Z}_8^* is not isomorphic to either of these.

Such an element is called a generator because it generates the whole group by just taking powers of it. For example, $1, 1 + 1, 1 + 1 + 1$, and $1 + 1 + 1 + 1$ give all the elements of \mathbb{Z}_4 .

Question Sheet 3

1. (a) The cosets are $\left\{ \left| \begin{array}{c} | \\ | \\ | \end{array} \right. \right\}$, $\left\{ \left| \begin{array}{c} \times \\ \times \\ | \end{array} \right. \right\}$, $\left\{ \left| \begin{array}{c} \times \\ \times \\ \times \end{array} \right. \right\}$, and $\left\{ \left| \begin{array}{c} \times \\ \times \\ \times \end{array} \right. \right\}$.
- (b) These cosets do not form a group like the cosets of $n\mathbb{Z}$ in \mathbb{Z} do (to give \mathbb{Z}_n). To see this, notice that the inverse of the first element in the second coset is itself (so it lives in the second coset), however the inverse of the second element in this coset is in the third coset. So it doesn't make sense to talk about the inverse of the second coset being one of the other cosets.
- (c) The condition on the subgroup is called being a **normal** subgroup, and this means that for any element $g \in G$, $gHg^{-1} = H$.

2. All the subgroups of \mathcal{Q}_8 are $\{1\}$, $\{1, -1\}$, $\{1, i, -1, -i\}$, $\{1, j, -1, -j\}$, $\{1, k, -1, -k\}$, and \mathcal{Q}_8 itself, which have orders 1, 2, 4, 4, 4, 8 respectively.

All the subgroups of $\text{Sym}(3)$ are $\left\{ \left| \begin{array}{c} | \\ | \\ | \end{array} \right. \right\}$, $\left\{ \left| \begin{array}{c} | \\ | \\ | \end{array} \right. \right\}$, $\left\{ \left| \begin{array}{c} \times \\ \times \\ | \end{array} \right. \right\}$, $\left\{ \left| \begin{array}{c} | \\ | \\ | \end{array} \right. \right\}$, $\left\{ \left| \begin{array}{c} | \\ | \\ | \end{array} \right. \right\}$, $\left\{ \left| \begin{array}{c} \times \\ \times \\ \times \end{array} \right. \right\}$, and $\text{Sym}(3)$ itself. These have orders 1, 2, 2, 3, 6 respectively.

3. The subgroup of $\text{Braid}(3)$ is the group that consists of all braids that start and end at the same spot. So $\left| \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \right|$ is in this subgroup but $\left| \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \right|$ is not.

4. *Proof.* Suppose $a^{-1}b \in H$. Then the coset $a^{-1}bH = H$ and so multiplying on the left by a we have $bH = aH$ and so a and b belong to the same coset.

On the other hand, if a and b are in the same coset, then $b = ah$ for some $h \in H$. Multiplying on the left by a^{-1} we have that $a^{-1}b = h$ and thus $a^{-1}b \in H$. ■

7. (a) *Proof.* Since the order of an element is the order of the subgroup generated by the element, and by Lagrange's theorem we know that the order of any subgroup must divide the order of a group, we can conclude that the order of an element must divide the order of the group it lives in. ■

- (b) *Proof.* First suppose $a \equiv 0$ in \mathbb{Z}_p . Then $a^p \equiv a \pmod{p}$. So we can assume $a \not\equiv 0 \pmod{p}$. Since p is a prime, a must be an element of \mathbb{Z}_p^* , so consider a in the group (\mathbb{Z}_p^*, \times) .

We know that the order of a must divide the order of the group, $p - 1$. We will now prove that $a^{p-1} \equiv 1 \pmod{p}$. Let the order of a be k , and since k divides $p - 1$, there is some integer n such that $kn = p - 1$. Then

$$a^{p-1} \equiv a^{kn} \equiv 1^n \equiv 1 \pmod{p}.$$

We now have that $a^{p-1} \equiv 1 \pmod{p}$, so multiplying both sides by a we get $a^p \equiv a \pmod{p}$, completing the proof. ■

8. (a) The possible orders for subgroups of \mathbb{Z}_{12} must be all the numbers that divide the order of the group (by Lagrange's theorem). Since the order is 12, the possible orders of subgroups are 1, 2, 3, 4, 6, and 12. In fact, we see that there do exist subgroups of each of these orders given by

$$\{0\}, \{0, 6\}, \{0, 4, 8\}, \{0, 3, 6, 9\}, \{0, 2, 4, 6, 8, 10\}, \text{ and } \mathbb{Z}_{12}$$

respectively.

- (b) In $(\mathbb{Z}_n, +)$, it turns out that for each k that divides n , there is exactly one subgroup of that order, which is pretty amazing!