Math 312/ AMS 351 (Fall '17)

Partial Solutions to Sample Questions for Midterm 2

1. Let $\pi, \sigma \in \Sigma_5$ be two permutations given by

$$\begin{aligned} \pi &= (12)(345) \\ \sigma &= (13)(24) \end{aligned}$$

   a) Compute $\pi\sigma$ and $\sigma\pi$.

   b) For each of the permutations $\pi, \sigma, \pi\sigma, \sigma\pi$ find the order and sign.

   Solution: What you need to know:

   - the order of a cycle of length n is n
   - the signature of a cycle of length n is $(-1)^{n-1}$ (i.e. odd for transpositions, even for length 3, etc.)
   - the oder of a product of disjoint cycles is the lcm of the lengths
   - if you view the signature as ± 1, the signature is multiplicative (i.e. odd+odd=even, even+even=even, odd+even=odd) – here you don't even need to have disjoint cycles.

   (Also good to know: the number of transposition in decomposing a permutation is of the same parity to the signature, i.e. even or odd depending on the signature)

   In the examples above, order of π is $lcm(2,3) = 6$, while for $\sigma = lcm(2,2) = 2$. The signature is $(-1) \cdot 1 = -1$ (odd) for π and even for σ.

3. Let G be a group and let c be a fixed element of G. Define a new operation '$*$' on G by
$$a * b = ac^{-1}b.$$
Prove that the set G is a group under $*$.

Solution: What you need to check is

- (associativity) $(x * y) * z = x * (y * z)$. Here we have
$$(x * y) * z = (xc^{-1}y) * z = (xc^{-1}y)c^{-1}z = xc^{-1}yc^{-1}z$$
Similarly
$$x * (y * z) = xc^{-1}(yc^{-1}z) = xc^{-1}yc^{-1}z$$
thus the same thing. (Note in the last step we are allowed to drop the () because we know that G is a group, and thus the multiplication is associative).
- (existence of a unit) I need e such that
$$x * E = E * x = x$$
Since $x * E = xc^{-1}e$, it is clear that I can take
$$E = c$$
as unit.
- (existence of inverse) Need to find y such that
$$x * y = y * x = E = c$$
This gives the equation for y
$$xc^{-1}y = c$$
We get
$$y = cx^{-1}c$$
(multiply by x^{-1} and then c to the left). Finally, we immediately check
$$y * x = E(= c)$$
showing that indeed y is the inverse of x (wrt to $*$).

4. Consider the group $U(9)(=\mathbb{Z}_9^*)$ of invertible congruence classes mod 9.

   a) Show that $U(9)$ is cyclic of order 6.

   b) Give an explicit isomorphism $(U(9),\cdot)\cong(\mathbb{Z}_6,+)$.

   Solution: $U(9)=\{1,2,4,5,7,8\}$ since $2^2=4$, $2^3=8$, $2^4=7$, $2^5=5$, and $2^6=1$, we see that the order of 2 in $(U(9),\cdot)$ is 6, thus the group is cyclic.

   To give an isomorphism from a cyclic group $C_n=\langle a\rangle=\{e,a,a^2,\dots,a^{n-1}\}$ to $\mathbb{Z}_n$, you only need to choose the generator a for C_n (i.e. an element of order n). Then the isomorphism is

$$\phi(a^j)=j\in\mathbb{Z}_n$$

   Concretely, in our example, we can take the generator $a=2$ (similarly we can $a=7$). The isomorphism will be given explicitly as follows

$$\phi:U(9)=\{1,2,4,5,7,8\}\to\mathbb{Z}_6=\{0,1,2,3,4,5\}$$

   by

$$\phi(1)=0,\ \phi(2)=1,\ \phi(4)=2,\ \phi(8)=3,\ \phi(7)=4,\ \phi(5)=5,$$

   (recall the general rule $\phi(2^j)=j$)

5. a) Prove that in any finite group, the number of elements of order 3 is even.

   b) Prove that any group of order 12 must contain an element of even order.

   c) Prove that any group of order 12 must contain an element of order 2.

Solution: Note that if x order 3, then x^2 has order 3 as well, and $x^{-1} = x^2$ (and $x \neq x^{-1}$). Clearly, I can group the elements of order 3 in pairs (x, x^{-1}) showing the number of order 3 elements is even.

(b) The possible orders in a group of order 12 are $1, 2, 3, 4, 6, 12$ (1 is only for the unit, thus we are left with $2, 3, 4, 6, 12$). There are $11 = 12 - 1$ non-unit elements in G. They can not be all of order 3 (from (a) the number of order 3 elements is always even). Thus, at least one of those 11 elements must have order $2, 4, 6, 12$, i.e. even order.

(c) Note the general fact: *if x has order n and $d \mid n$, then $y = x^{\frac{n}{d}}$ has order d.* In our situation, from (b), we know that there exists an element of even order, since $d = 2$ divides any even number, the conclusion follows. (e.g. x has order 6, then x^3 has order 2)

6. Let $G = D(6)$ be the group of symmetries of the regular hexagon.

   0) What is the order of G?

   a) Let R be the set of all rotations in G. Show that R is a subgroup of G. What is the order of R? Is R cyclic?

   b) Let $\sigma \in G$ be a reflection. Let $S = \langle \sigma \rangle$. What is the order of S?

   c) What are the possible orders $|H|$ of subgroups H in G? Are all the possible orders realized?

   d) Is there a cyclic subgroup of order 4 in G?

Solution: The order of the dihedral group $D(n)$ is $2n$. Thus in our situation, the order of G is 12.

The rotation form a cyclic subgroup. Namely if r is a primitive rotation (a rotation by $\frac{2\pi}{n}$), then

$$R = \langle r \rangle = \{e, r, r^2, r^3, r^4, r^5\}$$

(nothing to prove here, except to say: all rotations are powers of a basic rotation r, and thus R is cyclic.) The order of r (and $R = \langle r \rangle$) is 6.

Any reflection has order 2. Thus $S = \langle \sigma \rangle = \{e, \sigma\}$ has order 2.

Note that in a dihedral group, there are precisely n rotations (we consider e to be the trivial rotation) and n reflections. The reflections have order 2, while the rotations have order d where $d \mid n$ (e.g. in our situation r has order 6, r^2 has order 3 and r^3 has order 2). Thus, the possible orders that occur in $D(n)$ are 2 or d (divisors of n). In our situation the possible orders are

$$\{1, 2, 3, 6\}$$

Thus, we miss 4 (this answers item d)) and 12 ($D(12)$ is not cyclic.

The possible orders for H a subgroup of G are: $1, 2, 3, 4, 6, 12$. Clearly $1, 2, 3, 6$, we can take $H = \langle a \rangle$ cyclic. Order 12 also occurs: we can take $H = G$ (for any group G you always have 2 trivial subgroups: $\{e\}$ and G, thus the maximal order is always realized, but not for a cyclic subgroup). It remains to produce a subgroup of order 4. This is possible in this case: take σ_1 and σ_2 two reflections such that the axes of reflection are perpendicular on each other. This assumption will imply $\sigma_1\sigma_2 = \sigma_2\sigma_1$. Then

$$H = \{e, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$$

is a subgroup of order 4 of G. In conclusion, all orders allowed by Lagrange occur as orders of subgroups H in G.

7. Consider the groups $\mathbb{Z}_2 \times \mathbb{Z}_4$, $D(3)$, $\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_6$, $U(5)$, Σ_3, $\mathbb{Z}_8$, $\mathbb{Z}_4$. Find the odd one out. **Solution:**

   - $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$
   - $U(5) \cong \mathbb{Z}_4$
   - $D(3) \cong \Sigma_3$
   - $\mathbb{Z}_2 \times \mathbb{Z}_4 \ncong \mathbb{Z}_8$ ($\mathbb{Z}_8$ is cyclic, thus it has an element of order 8, while the maximal order in $\mathbb{Z}_2 \times \mathbb{Z}_4$ is 4)

8. True or False or Complete

- The positive integers (wrt addition) form a group. **F** (the inverses would be negative numbers)
- The set of square matrices of size n is a group with respect to **matrix multiplication**.
- In a group $(ab)^{-1} = \mathbf{b^{-1}a^{-1}}$
- In an abelian group, $(ab)^2 = a^2b^2$. **T**
- $(\mathbb{Z}_5, \cdot)$ is an abelian group. **F** (not a group; 0 is not invertible)
- Any group with 6 elements contains an element of order 6. **F** (if G contains an order 6 element, G is cyclic. But Σ_3 is an order 6 which is not cyclic - not even abelian)
- A group with 24 elements might contain a subgroup of order 10. **F** (Lagrange's Theorem)
- If G contains an element a of order $|G|$, then G is **cyclic**.
- The Chinese Remainder Theorem implies that $\mathbb{Z}_4 \times \mathbb{Z}_6 \cong \mathbb{Z}_{24}$. **F** (need relatively prime indices, e.g. $\mathbb{Z}_3 \times \mathbb{Z}_8 \cong \mathbb{Z}_{24}$)
- The number of invertible elements in $\mathbb{Z}_{24}$ is $\phi(\mathbf{24}) = \phi(\mathbf{8})\phi(\mathbf{3}) = (\mathbf{8} - \mathbf{4})(\mathbf{3} - \mathbf{1}) = \mathbf{8}$.
- A group of oder 4 is always abelian. **T** (there are two groups of order 4: $\mathbb{Z}_4$ (cyclic gp.) and $\mathbb{Z}_2 \times \mathbb{Z}_2$ (Klein gp.))

Note: For the exam, T/F suffices (no explanation needed)