MATH-F410 – REP. DES GROUPES & APP. A LA PHYS.

Solutions des exercices 2023-2024

Séance 1 : Groupes finis d'ordre ≤ 7, théorème de Cayley, théorème de Lagrange

1. Finite groups of order 4

Section a)

Let $G = \{e, a_1, a_2, a_3\}$ be a group of order 4. Take two different elements a_1 and a_2 different from the identity. Then, multiplying by the inverses on the left and right:

$$a_1 \cdot a_2 = a_1 \Rightarrow a_2 = e \ , \qquad\qquad a_1 \cdot a_2 = a_2 \Rightarrow a_1 = e \ .$$

We conclude that $a_1 \cdot a_2$ is neither a_1 or a_2. It must be either e or a_3:

1. If $a_1 \cdot a_2 = e$, the elements commute because $a_2 = a_1^{-1}$.
2. If $a_1 \cdot a_2 = a_3$, redo the argument starting from the product $a_2 \cdot a_1$. The only possibility is $a_2 \cdot a_1 = a_3$, and thus the elements commute.

We have shown that any two elements of an order 4 group commute, so the group is necessarily Abelian.

Section b)

We will use the fact that in the multiplication table, each element appears once and only once in each row or column – show that this is the case, it's easy! We don't write the row and column associated with the identity since these are redundant ($e \cdot g = g \cdot e = g$ for any $g \in G$). We start filling the table and we have two options picking an element $a_1 \neq e$, either $a_1 \cdot a_1 = e$ or $a_1 \cdot a_1 = a_2$ for some $a_2 \neq e$ (a_2 is just a label for an element not equal to e!). By now we have then the following options:

	a_1	a_2	a_3
a_1	a_2	?	?
a_2	?	?	?
a_3	?	?	?

	a_1	a_2	a_3
a_1	e	?	?
a_2	?	?	?
a_3	?	?	?

1. On the left, $a_1 \cdot a_2$ can be either e or a_3. If it's e, then necessarily $a_1 \cdot a_3 = a_3$, which would imply $a_1 = e$. This cannot be, therefore the only option is $a_1 \cdot a_2 = a_3$, and $a_1 \cdot a_3 = e$. The other products follow by the ones of a_1 knowing now that $a_2 = a_1^2$, and $a_3 = a_1^3$.

2. On the right, $a_1 \cdot a_2$ can be either a_2 or a_3. If it's a_2 it would mean $a_1 = e$, and since this cannot be it must be $a_1 \cdot a_2 = a_3$. This, in turn, implies $a_1 \cdot a_3 = a_2$. The table is symmetric due to the group being Abelian, so this fixes the first column also.

The situation is then the following:

	a_1	a_2	a_3
a_1	a_2	a_3	e
a_2	a_3	e	a_1
a_3	e	a_1	a_2

	a_1	a_2	a_3
a_1	e	a_3	a_2
a_2	a_3	?	?
a_3	a_2	?	?

You can fill in the table on the right with $a_2 \cdot a_2 = a_1$, but then $a_2 \cdot a_3 = e$ and you realize that both tables are isomorphic (just go from left to right by moving the rows down and renaming the elements). So the only real different possibility is $a_2 \cdot a_2 = e$, $a_2 \cdot a_3 = a_1$. We conclude that there are two possible groups of order 4 ($\mathbb{Z}_4$ and the so called Klein four-group):

	a_1	a_2	a_3
a_1	a_2	a_3	e
a_2	a_3	e	a_1
a_3	e	a_1	a_2

	a_1	a_2	a_3
a_1	e	a_3	a_2
a_2	a_3	e	a_1
a_3	a_2	a_1	e

Section c)

The key idea to write the previous groups as subgroups of S_4 is viewing the rows of the previous tables in two ways. One, as left actions of the group on itself. As an example, the first row on the left would be the action of L_{a_1}: $L_{a_1}(e) = a_1$, $L_{a_1}(a_1) = a_2$, $L_{a_1}(a_2) = a_3$, and $L_{a_1}(a_3) = e$. The other way to look at this row is as a permutation, $(1\,4\,3\,2)$ acting on the top row (in which you imagine to add e on the left): $(1\,4\,3\,2)(e\,a_1\,a_2\,a_3) = (a_1\,a_2\,a_3\,e)$. This identifies left actions (which are by themselves identified with the group elements) with permutations. In this way, we conclude:

$$\mathbb{Z}_4 \cong \{e, (1\,4\,3\,2), (1\,3)(2\,4), (1\,2\,3\,4)\}\ ,$$
$$V \cong \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}\ ,$$

where V is the Klein four-group (the table on the right). You can check this is correct by reproducing the multiplication tables using the permutations! Also, there are more subgroups of S_N isomorphic to $\mathbb{Z}_4$, we only found *one* easily obtained from our table. You can try to find all of them (there are three) and think of how you would obtain them from relabelling the table...

2. Cayley's theorem

Section a)

Let us clarify a bit the nomenclature because it is not completely clear in the question. When we have a subgroup of S_n, we say it is a regular group of permutations if all the elements of the subgroup which are not the identity act nontrivially on every element of the set $\{1, \ldots, n\}$. As an example, $\{e, (1\,2\,3), (1\,3\,2)\}$ is a regular subgroup of S_3, but $\{e, (1\,2)\}$ is not (although this last group, since it is equal to S_2, would be regular if we think of it as a subgroup of S_2). Let $G \subseteq S_n$ be a regular group of permutations. Assume one element g has a decomposition into disjoint cycles in which there are two cycles of different length,

$$g = (a_1 \ldots a_m)(b_1 \ldots b_n) \ldots \ ,$$

with $m < n$. There is a key property of cycles of length p now, you can convince yourselves that:

$$(c_1 \ldots c_p)^k \neq e \quad \text{if } 1 \leq k \leq p-1 \ , \qquad\qquad (c_1 \ldots c_p)^p = e \ ,$$

which also shows $(c_1 \ldots c_p)^{-1} = (c_1 \ldots c_p)^{p-1}$. Then, since the cycles in g are disjoint:

$$g^m = (a_1 \ldots a_m)^m (b_1 \ldots b_n)^m \ldots = (b_1 \ldots b_n)^m \ldots \ ,$$

and this is not the identity (because it acts nontrivially on any b_i) but acts trivially on any of the a_i. This cannot be part of a regular group of permutations. We conclude then that the decomposition into disjoint cycles of any g in a regular group of permutations has to produce cycles of equal length.

Section b)

Consider a group of prime order p. By Cayley's theorem, we can view it as a subgroup of S_p, and in this way it is a regular group of permutations. Any permutation in this subgroup different from the identity, by the previous section, has to be decomposed into a product of cycles of equal length. Call c one of these permutations; since it has to modify the p elements and p is prime, the only possible decomposition into elementary cycles is one cycle of length p (because the sum of the lengths of all the cycles has to add up to p, and if cycles have to be of equal length $l > 1$ this means that $nl = p$, with n the number of cycles. For p prime, the only solution is $l = p, n = 1$). But then we know that the sequence of powers of c produces by itself the p elements of the group: $c \neq c^2 \neq c^3 \neq \ldots \neq c^p = e$. The group is then necessarily the cyclic group $\mathbb{Z}_p$, which is Abelian. Let us repeat the punchline: for p prime, there is a single group of order p, the cyclic group $\mathbb{Z}_p$.

3. Finite groups of order 6

Section a)

Recall that the (left) cosets are sets obtained by multiplying the elements of H by elements $g \in G$, we denote them as gH. The following statements hold:

- No coset is empty, since H is not empty (it is a subgroup so it contains at least the identity).
- Every element of G is in at least one coset. This is a consequence of $e \in H$, which implies $g = ge \in gH$ for any $g \in G$.
- If two cosets intersect, they are the same. To prove this, take gH and $g'H$ with non-vanishing intersection, and pick $\bar{g} \in gH \cap g'H$. We show $gH \subset g'H$ as follows. Take $k \in gH$, so that $k = gh_k$ for some $h_k \in H$. Since $\bar{g} \in gH$, $\bar{g} = gh_{\bar{g}}$ as well, and then $k = \bar{g}h_{\bar{g}}^{-1}h_k$. But $\bar{g} \in g'H$, so $\bar{g} = g'h'_{\bar{g}}$ and $k = g'h'_{\bar{g}}h_{\bar{g}}^{-1}h_k \in g'H$. This shows $gH \subset g'H$; the converse is analogously true and we conclude $gH = g'H$.

These three statements together show that (left) cosets form a partition of G: they are a family of subsets of G which are non-empty, their union covers G, and the intersection of any two distinct cosets is empty. Furthermore, all of them have equal number of elements $|H|$. This is a consequence of the fact that in gH there is one element for each H element: it is not possible to have $gh = gh'$ for $h \neq h'$. All in all, the number of elements in G (denoted $|G|$) is equal to the number of cosets times $|H|$. Thus, $|H|$ divides $|G|$.

Section b)

By the previous section, a group of order 6 can only have non-trivial subgroups of order 3 or 2 (the other divisors of 6 are 6 and 1, but these are the trivial subgroups corresponding to the full group or the group formed by only the identity). For order 3, the only possible group is $\mathbb{Z}_3$; and similarly for order 2 it is only $\mathbb{Z}_2$. So the non-trivial subgroups, if any, are $\mathbb{Z}_2$ or $\mathbb{Z}_3$. These cyclic groups are generated by a single element, which we multiply until we go back to the identity. Let a be an element of our group of order 6 such that there is no other element with higher order. The possibilities are.

- a has order 6, so $a \neq a^2 \neq a^3 \neq a^4 \neq a^5 \neq a^6 = e$. The group is then $\mathbb{Z}_6$.
- a has order 3, so it forms a $\mathbb{Z}_3$ subgroup, $\{a, a^2, a^3 = e\}$. Take an element b not in this $\mathbb{Z}_3$ subgroup. Neither ba nor ba^2 can be in the subgroup (otherwise b would be as well), so the full group is $\{e, a, a^2, b, ba, ba^2\}$. You can try to fill in the full multiplication table now. The key ingredients we do not yet have are the values of b^2 and of ab. For b^2, it is either $b^2 = e$ or b would have order 3 (it cannot have order 6 by assumption). If it had order 3, then b^2 clearly cannot be e, b, ba, ba^2 and the only options are a or a^2. If it were $b^2 = a$, then $ba = a^3 = e$, and this cannot happen because b is not in the $\mathbb{Z}_3$ generated by a. Show analogously that b^2 cannot be a^2; the conclusion is that b must have order 2, and so $b^2 = e$. Now, for ab, it is easy to check that it cannot be e, a, a^2, b. If $ab = ba$, we would get $(ab)^2 = a^2b^2 = a^2$ and $(ab)^3 = a^3b^3 = b$ just using the previous known products. But this cannot happen because then ab would have order larger than 3. We conclude $ab = ba^2$. The full table is written below.
- a has order 2, so there is a $\mathbb{Z}_2$ subgroup $\{a, a^2 = e\}$, and there can be no element with order higher tan two by assumption. Taking b outside of the previous $\mathbb{Z}_2$, it

must be $b^2 = e$ then. Take ba now. Since $ba \neq e$ (otherwise $b = a$), again we must have $(ab)^2 = e$ so that its order is not higher than 2. Also, $ba = ab$ multiplying by a on the left and right. We have 4 elements until now, we need something else to get a group of order 6, so we introduce c different from a, b, ab and forming another $\mathbb{Z}_2$, $c^2 = e$. By the same argument as above, $ac = ca$ and $bc = cb$ are new elements, but this cannot happen because we would have 7 elements. Therefore there must be at least an order 3 element.

	a	a^2	a^3	a^4	a^5
a	a^2	a^3	a^4	a^5	e
a^2	a^3	a^4	a^5	e	a
a^3	a^4	a^5	e	a	a^2
a^4	a^5	e	a	a^2	a^3
a^5	e	a	a^2	a^3	a^4

	a	a^2	b	ba	ba^2
a	a^2	e	ba^2	b	ba
a^2	e	a	ba	ba^2	b
b	ba	ba^2	e	a	a^2
ba	ba^2	b	a^2	e	a
ba^2	b	ba	a	a^2	e

Table 1: The two order 6 groups obtained above, the first one has an order 6 element and it is therefore $\mathbb{Z}_6$, the second one has an order 3 element a and an order 2 one, b, as basic building blocks. Notice it is non-Abelian. This group is the dihedral group D_3, which turns out to be isomorphic to S_3 (see below).

Section c)

$\mathbb{Z}_6$ is Abelian, while S_3 is not, so the only candidate is the group in the second table above. You can indeed show that the following is an isomorphism from the second group above into S_3:

$$e \hookrightarrow e \qquad a \hookrightarrow (1\,2\,3) \qquad a^2 \hookrightarrow (1\,3\,2)$$
$$b \hookrightarrow (1\,2) \qquad ba \hookrightarrow (2\,3) \qquad ba^2 \hookrightarrow (1\,3)$$

Check the product table is reproduced by doing the products within S_3.

Section d)

$\mathbb{Z}_2 \times \mathbb{Z}_3$ is Abelian (product of Abelian groups), so it must be $\mathbb{Z}_6$. To make the identification with the first of the tables above, call $\mathbb{Z}_2 = \{p, p^2 = e\}$ and $\mathbb{Z}_3 = \{q, q^2, q^3 = e\}$. Then, define $a = (p, q)$ in the product group $\mathbb{Z}_2 \times \mathbb{Z}_3$. This satisfies:

$$a^2 = (e, q^2) \qquad a^3 = (p, e) \qquad a^4 = (e, q) \qquad a^5 = (p, q^2) \qquad a^6 = (e, e) = e\ ,$$

which indeed reproduces the $\mathbb{Z}_6$ table found above.

Section d)

This is done via Burnside's theorem, which will be extensively reviewed in the following exercise sheets. It says that the order of a finite group coincides with the sums of the squares of the dimensions of the irreducible representations. In this case we have order 6

groups, and one always present irreducible representation is the trivial one with dimension 1, so:

$$6 = 1 + \sum_i n_i^2 \ ,$$

where the n_i are positive integers giving the dimensions of the non-trivial irreps. This has only two possible solutions:

- $n_i = 1$ for $i = 1, \ldots, 5$. In addition to the trivial representation, there are 5 non-trivial 1-dimensional ones.
- $n_1 = 1$, $n_2 = 2$. In addition to the trivial representation, there is another non-trivial one which is 1-dimensional, and a 2-dimensional one.

We will not discuss here in detail what happens for each of the groups above. You can however anticipate that the 2-dimensional irreducible representation will happen for the group $S_3 \cong D_3$, because the dihedral group D_3 is given by rotations and reflections in the plane (2-dimensional matrices then) that leave an equilateral triangle invariant.

4. Regular representations of groups of order 4

First a review of notation. The regular representation of a finite group G of order $|G| = n$ can be thought to act on $L^2(G) = \{f : G \to \mathbb{C}\}$. This is a complex vector space of dimension n, since any function f on G can be written as:

$$f = \sum_{g \in G} f(g) E_g \ ,$$

where we have defined for each $g \in G$ the function $E_g : G \to \mathbb{C}$ / $E_g(h) = \delta_{g,h}$ $\forall h \in G$. The set $\{E_g \ / \ g \in G\}$ is the canonical basis of $L^2(G)$, we will always use it unless otherwise explicitly stated. The regular representation of the group G defines then a linear map in $L^2(G)$ for each $g \in G$, $T_R(g) : L^2(G) \to L^2(G)$ as:

$$T_R(g) f : G \to \mathbb{C} \ , \quad (T_R(g) f)(h) = f(hg) \qquad \forall f \in L^2(G)$$

It is useful for future reference to understand how the regular representation acts on the canonical basis of $L^"(G)$ described above. This is seen as follows:

$$(T_R(g) E_{g'})(h) = E_{g'}(hg) = \delta_{g',hg} = \delta_{g'g^{-1},h} = E_{g'g^{-1}}(h) \ ,$$

for any $g, g', h \in G$. We conclude that $T_R(g) E_{g'} = E_{g'g^{-1}}$. This is all we need to identify the regular representations of the groups of order 4, which recall are $\mathbb{Z}_4$ and the Klein group V (exercise 1).

For $\mathbb{Z}_4$, the previous equation shows that, being a the basic element of order 4:

$$T_R(a) E_e = E_{a^3} \ , \qquad T_R(a) E_a = E_e \ , \qquad T_R(a) E_{a^2} = E_a \ , \qquad T_R(a) E_{a^3} = E_{a^2} \ .$$

You can similarly find the action of the other elements $T_R(a^2)$, $T_R(a^3)$ ($T_R(e)$ acts as the identity always); or you can just obtain it by repeated application of $T_R(a)$ and using that the group structure is respected in the representation, so, *e.g.*, $T_R(a^2) = T_R(a)T_R(a)$. We will give the results as matrices written in the canonical basis of $L^2(G)$. Recall that the matrix representation of a linear map has in each *column* the components of the image of the corresponding basis element. We thus obtain, for $\mathbb{Z}_4$:

$$T_R(e) = \mathbb{I}\ , \qquad T_R(a) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}\ ,$$

$$T_R(a^2) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}\ , \qquad T_R(a^3) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}\ .$$

The result for the Klein group is totally analogous, but we have to use the corresponding group multiplication table (recall there are two basic order 2 elements which we will call a and b, $a^2 = b^2 = e$, and then their product $ab = ba$ which also satisfies $(ab)^2 = e$. You can make contact with exercise 1 relabelling $a = a_1$, $b = a_2$, $ab = a_3$). You should find:

$$T_R(e) = \mathbb{I}\ , \qquad T_R(a) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\ ,$$

$$T_R(b) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}\ , \qquad T_R(ab) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}\ .$$

A couple of comments. Notice that these matrices are unitary, as they should be since the regular representation is unitary (for the *mean* scalar product, in which elements of the canonical basis of $L^2(G)$ are orthogonal). Also, notice that these are just permutation matrices: if you think of them acting on a 4-component vector, they reshuffle the components. It is then immediate to read from here the embedding of each of the groups as a subgroup of S_4.

5. Center of a group

One important thing here is to realize that, before proving that a certain subset of a group is normal, we have to check it is a subgroup. Take $Z(G) = \{h \in G \,/\, hg = gh\ \forall g \in G\}$:

- $e \in Z(G)$, since the identity trivially commutes with all elements of a group.

- Given $h \in Z(G)$, by definition of the center $hg = gh$ for any $g \in G$. Multiply by h^{-1} the previous equation on the left and on the right to obtain $gh^{-1} = h^{-1}g$ (again, for any $g \in G$). We conclude $h^{-1} \in Z(G)$.
- For $h, h' \in Z(G)$, consider the product hh'. For any $g \in G$, since both h and h' commute with all elements of the group, we have $hh'g = hgh' = ghh'$. Thus, $hh' \in Z(G)$.

The previous three statements guarantee that $Z(G)$ is a subgroup if G (associativity is inherited from the product in G). We can show now that it is normal by proving that left and right cosets coincide. Given $g \in G$:

$$gZ(G) = \{gh \ / \ h \in Z(G)\} = \{hg \ / \ h \in Z(G)\} = Z(G)g \ .$$