ENGINEERING MATHEMATICS - TUTORIAL AND HOMEWORK 5

Please submit all exercises below in hard copy (either in English or in Hebrew) next Thursday, December 3^{rd}, in the tutorial. Sections marked as bonus are not mandatory.

1. The symmetric group

1.1. Definition: Let X be a set. We define the group $Sym(X)$ to be the set of all one to one and onto functions from X to X, with function composition.

Remark: one easily sees that indeed $Sym(X)$ is a group, with the identity function on X being the neutral element (make sure you understand that function composition is indeed associative and that moreover any one to one and onto function has an inverse).

1.2. Notation: If $X = \{1, 2, ..., n\}$ we denote $S_n := Sym(X)$. S_n is the group of permutations of n elements (make sure you understand why $ord(S_n) = n!$). We denote the invertible function $\sigma : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$ by

$$\begin{pmatrix} 1 & 2 & 3 & . & . & n \\ \sigma(1) & \sigma(2) & \sigma(3) & . & . & \sigma(n) \end{pmatrix} \in S_n,$$

e.g. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$ is the permutation that switches between the first and the second elements, and does nothing to the third.

1.3. Cycles notation: Sometimes it is easier to use cycles notation: by $(i_1 i_2 i_3 ... i_k)$ we mean the permutation that sends i_1 to i_2, i_2 to i_3,...,i_{k-1} to i_k and i_k to i_1 (and does nothing to all other elements). For instance $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$ will also be denoted by (12). Note that if two cycles $(i_1 i_2 i_3 ... i_k)$ and $(j_1 j_2 j_3 ... j_l)$ contain no common element (i.e. for any $n \in \{1, 2, 3..., k\}$ and any $m \in \{1, 2, 3, ..., l\}$: $i_n \neq j_m$) then they commute (i.e. $(i_1 i_2 i_3 ... i_k)(j_1 j_2 j_3 ... j_l) = (j_1 j_2 j_3 ... j_l)(i_1 i_2 i_3 ... i_k)$).

1.4. Remark: Any permutation can be written in a cycles notation. Working through this work sheet you should be convinced of this fact.

1.5. Example: In S_5 we have ((12)(34)) is the permutation switching the first and the second elements, switching the third and the fourth elements, and does nothing to the fifth. The permutation (1524) sends the first element to the fifth, the fifth to the second, the second to the fourth, the fourth to the first, and does nothing to the third. We may calculate:

$$((12)(34))(1524) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix} = (15)(234),$$

but

$$(1524)((12)(34)) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} = (143)(25),$$

hence S_5 is not commutative (not Abelian).

Date: November 26^{th} 2015.

1.6. Claim: S_n is commutative if and only if $n = 2$.

Proof: $S_2 = \{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$. As it has only one element which is not the identity function (the neutral element of the group), and as any element commute with itself and with the neutral element, then all elements commute, i.e. S_2 is commutative.

Now assume $n > 2$. Take $\sigma = (12) \in S_n$ and $\tau = (23) \in S_n$. One may calculate $\sigma\tau = (123)$ but $\tau\sigma = (132)$, hence σ and τ do not commute, and S_n is not commutative. □

1.7. Exercise: Prove that any non-Abelian group has order at least 6, i.e. we may think of S_3 as the "smallest" non-Abelian group (hint: starting with a non-Abelian group G you have $a, b \in G$ such that $ab \neq ba$. You may now prove that all the elements in the set $\{1_G, a, b, ab, ba, aba\} \subset G$ are different. If you get stuck in the middle try to use what you already proved and say something about the order of the element a).

1.8. We naturally think of the group of permuting n elements (S_n) as a subgroup of the group of permuting $n+1$ elements (S_{n+1}). However this is not accurate: a group morphism which is one to one is called an embedding. We may find many group morphisms from S_n to S_{n+1} that are one to one, i.e. there are many ways to embed S_n inside S_{n+1}. Let us explain:

A general element $\sigma \in S_n$ may be written as $\begin{pmatrix} 1 & 2 & 3 & . & . & n \\ \sigma(1) & \sigma(2) & \sigma(3) & . & . & \sigma(n) \end{pmatrix}$. So we can send it to $\begin{pmatrix} 1 & 2 & 3 & . & . & n & n+1 \\ \sigma(1) & \sigma(2) & \sigma(3) & . & . & \sigma(n) & n+1 \end{pmatrix} \in S_{n+1}$. In other word we define a map $\phi : S_n \to S_{n+1}$ that says "permute the first n elements like you should have if the last one was not there, and leave the last one untouched".

Now note that another map would be to send σ to $\begin{pmatrix} 1 & 2 & 3 & . & . & n & n+1 \\ 1 & \sigma(1)+1 & \sigma(2)+1 & \sigma(3)+1 & . & . & \sigma(n)+1 \end{pmatrix} \in S_{n+1}$. This is a map $\phi' : S_n \to S_{n+1}$ that says "permute the last n elements like you should have if the first one was not there, and leave the first one untouched".

1.9. Exercise: Prove that ϕ defined above is indeed a group morphism, and that it is indeed one to one (hint: it may seems difficult but once you understand what is going on it is very easy to show that all the axioms of a group morphism hold. In order to show ϕ is one to one find an inverse function from the image of ϕ back to S_n - note that this is not a function from all of S_{n+1}, but only from the subset of S_{n+1} defined by $\{\sigma \in S_{n+1} | \exists \tau \in S_n : \phi(\tau) = \sigma\}$). This subset is a subgroup of S_{n+1} (this is true in general - the image of any group homomorphism is a subgroup of the range, it is an easy exercise you do not have to do).

1.10. Exercise: let $m < n$ be two natural numbers. Assume that $\psi : S_m \to S_n$ is a one to one group morphism (i.e. ψ is an embedding of S_m into S_n). Let $\mu \in S_n$ be any element. Prove that $\psi' : S_m \to S_n$ defined by: $\forall \tau \in S_m : \psi'(\tau) = \mu^{-1}\psi(\tau)\mu$ is an embedding as well (i.e. ψ' is a one to one group morphism).

1.11. Example: let us show that starting from one embedding in 1.10 we may get a different one: we take $\psi : S_2 \to S_3$ given by $\psi(\tau) = \begin{pmatrix} 1 & 2 & 3 \\ \tau(1) & \tau(2) & 3 \end{pmatrix}$, and $\mu \in S_3$ given by $\mu = (13)$ (i.e. the permutation switching between the first and third elements and does nothing to the second). We want to calculate for any $\tau \in S_2$: $\psi'(\tau) = \mu^{-1}\psi(\tau)\mu$. First we note that $\mu^{-1} = \mu$, so we need to calculate $\psi'(\tau) = \mu\psi(\tau)\mu = (13)\psi(\tau)(13)$. As S_2 contains only two elements (the identity and (12)) we calculate both straight forward:

$$\psi'(1_{S_2}) = (13)\begin{pmatrix} 1 & 2 & 3 \\ 1_{S_2}(1) & 1_{S_2}(2) & 3 \end{pmatrix}(13) = (13)\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}(13) = 1_{S_3},$$

$$\psi'((12)) = (13)\psi((12))(13) = (13)\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}(13) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23).$$

But $\psi((12)) = (12) \in S_3$, thus $\psi \neq \psi'$, i.e. these are two different embeddings of S_2 into S_3. Note that this example is a special case of 1.8.

Remark: we saw that S_n may be embedded in S_{n+1} in many different ways, and hence S_n is not a subgroup of S_{n+1} in a canonical way. This is very similar to the fact that $\mathbb{R}$ may be embedded in $\mathbb{R}^2$ (as vector spaces) in many different ways, and hence $\mathbb{R}$ is not a subspace of $\mathbb{R}^2$ in a canonical way.

2. Transpositions and the sign of a permutation

Recall the commutative group of residues modulo 2 with addition: the set $\{\bar{0}, \bar{1}\}$ and the operation is $\bar{0} + \bar{0} = \bar{1} + \bar{1} = \bar{0}, \bar{0} + \bar{1} = \bar{1}$. We denote this group by $\mathbb{Z}/2\mathbb{Z}$.

2.1. Definition: a cycle in S_n of length 2 is called a transposition (i.e. if $i_1, i_2 \in \{1, 2, .., n\}$ and $i_1 \neq i_2$ then $(i_1 i_2) \in S_n$ is a transposition - it switches i_1 and i_2 and does nothing to all other elements).

2.2. Theorem: Any permutation $\sigma \in S_n$ can be presented as a composition of finitely many transpositions. This presentation is not unique, however the parity of the number of transpositions is unique, i.e. if $\sigma = \Pi_{i=1}^{n}(a_i b_i) = \Pi_{j=1}^{m}(c_j d_j)$ then $n - m \equiv 0 \ (mod\ 2)$.

Remark: (1) As always we define the composition of zero transpositions to be the identity element of S_n (the permutation that does nothing). (2) We will not prove Theorem 2.2 in this course, however you may use it.

2.3. Definition: we define a function $sgn : S_n \to \mathbb{Z}/2\mathbb{Z}$ by $sgn(\sigma) = \bar{0}$ if σ can be presented as a composition of an even number of transpositions, and $sgn(\sigma) = \bar{1}$ if σ can be presented as a composition of an odd number of transpositions. By Theorem 2.2 this function is well defined.

2.4. Exercise: prove that $sgn : S_n \to \mathbb{Z}/2\mathbb{Z}$ is a group homomorphism.

3. Motivation

In the future we will see some examples where the groups S_n are extremely useful (e.g. when we will introduce the Determinant function). The main importance of these groups when we discuss abstract algebra and Group Theory in general is the following theorem:

3.1. Cayley's Theorem: For any finite group G there esixts $n \in \mathbb{N}$ such that G is isomorphic (a group isomorphism) to a subgroup of S_n.

3.2. Exercise: (bonus) Let us prove Cayley's Theorem: we define a map $\phi : G \to Sym(G)$ (in $Sym(G)$ we consider G as a set, and forget it has a group structure) by $\phi(g) = \sigma_g \in Sym(G)$, where $\sigma_g(h) := g * h \in G$ (for any $h \in G$). Prove that ϕ is a group homomorphism, and that it is one to one. Thus G is isomorphic to $\phi(G)$ (the image of G under ϕ), and $\phi(G)$ is a subgroup of $Sym(G)$ (this is true in general - the image of any group homomorphism is a subgroup of the range, it is an easy exercise). Finally taking n to be $ord(G)$ we have $Sym(G) = S_{ord(G)} = S_n$, and we are done.

3.3. Exercise: (bonus) We saw that $\mathbb{Z}/N\mathbb{Z}$ (the set of residues modulo N with addition modulo N) is an Abelian group. Find a subgroup of S_N that is isomorphic to $\mathbb{Z}/N\mathbb{Z}$ (hint: use the fact that $\mathbb{Z}/N\mathbb{Z}$ is cyclic).

Remark: solving bonus exercises 3.2 and 3.3 is independent, you do not need one in order to solve the other. I highly recommend to solve 3.2 - although it is not hard it has great importance, both mathematically and historically.

E-mail address: `ary.shaviv@weizmann.ac.il`