ENGINEERING MATHEMATICS - TUTORIAL AND HOMEWORK 4

Please submit all exercises below in hard copy (either in English or in Hebrew) next Thursday, November 26^{th}, in the tutorial. Sections marked as bonus are not mandatory.

1. Groups

1.1. Definition: A set G together with a map $* : G \times G \to G$ is called a group if the following properties hold:

(1) $\forall g_1, g_2, g_3 \in G : (g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ (associativity)
(2) $\exists e \in G$ such that $\forall g \in G : e * g = g * e = g$ (existence of a neutral element)
(3) $\forall g \in G \ \exists g' \in G$ such that $g * g' = g' * g = e$ (existence of inverse element)

Claim: $\forall g \in G \ \exists! g' \in G$ such that $g * g' = g' * g = e$.

Proof: by (3) above such g' exists, thus it is enough to show uniqueness: assume also g'' satisfies the equality, then using both (1) and (2) we have $g' = g' * e = g' * (g * g'') = (g' * g) * g'' = e * g'' = g''$. □

Remark: by a similar proof one gets that the neutral element is unique (make sure you understand).

Notation: the inverse element of g is usually denoted by g^{-1} and the neutral element by 1_G, or just 1 if G is clear from the context.

Definition: let G be a group. G is called commutative (or Abelian) if the operation $*$ is commutative, i.e. if $\forall g_1, g_2 \in G : g_1 * g_2 = g_2 * g_1$. In that case we often denote the map $*$ by $+$, the inverse element of g by $-g$ and the neutral element by 0_G, or just 0.

Examples:

(1) $\mathbb{Z}$ with addition is an Abelian group.
(2) the residues modulo N ($\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, ..., \overline{N-1}\}$) with addition modulo N is an Abelian group (we denote this group by $\mathbb{Z}/N\mathbb{Z}$).
(3) $\mathbb{Z}$ with multiplication is not a group. Proof: if it was then $1_G * 1_G = 1_G$, i.e. 1_G satisfies the equation $a^2 = a$ so it is either 0 or 1. If it is 0 then $0 \cdot 7 = 7$, a contradiction. If it is 1 then there exists $0^{-1} \in \mathbb{Z}$ such that $0 \cdot 0^{-1} = 1$, a contradiction.
(4) any field (for instance $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$) with multiplication is an not a group (the proof is similar to the previous case - make sure you understand it).
(5) the residues modulo N with multiplication modulo N is not a group (the proof is similar to case (3) - make sure you understand it).

1.2. Exercise: Check which of the following structures are groups. If it is a group show that all the axioms hold, provide the neutral element, explain how to find the inverse to

Date: November 17^{th} 2015.

each element of the group and prove whether this group is Abelian or not. If it is not a group prove it (it is enough to show that one of the axioms does not hold).

(1) The set of integers divisible by 7, with addition.
(2) The set of all non-zero complex numbers, with multiplication.
(3) The set of integers having residue 1 modulo 7, with multiplication.
(4) The set of rotations with respect to a point O on the plane, with the usual composition.
(5) The set of 2-by-2 complex matrices $Mat_{2\times 2}(\mathbb{C})$ with matrix addition.
(6) The set of 2-by-2 complex matrices $Mat_{2\times 2}(\mathbb{C})$ with matrix mutliplication.
(7) The set of finite strings one can build from the English Alpha Bet with concatenation (i.e. $dog*cat = dogcat$). Note that formally the empty set (the string built from nothing) is such a string.

1.3. Exercise: denote the set of all invertible residues mod N by $(\mathbb{Z}/N\mathbb{Z})^\times$ (i.e. $(\mathbb{Z}/N\mathbb{Z})^\times := \{\bar{a} \in \{\bar{0},\bar{1},\bar{2},\bar{3},...,\overline{N-1}\} | \exists \bar{b} \in \{\bar{0},\bar{1},\bar{2},\bar{3},...,\overline{N-1}\} : \bar{a}\cdot\bar{b} = \bar{1}\}$). Prove that $(\mathbb{Z}/N\mathbb{Z})^\times$ with multiplication mod N is a group. Note you not only have to show all the axioms of 1.1, but to show that indeed multiplication mod N is a map from $(\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$ to $(\mathbb{Z}/N\mathbb{Z})^\times$, i.e. that if two residues are invertible mod N so does their multiplication mod N.

Definition: if G has finitely many elements the number of elements in it is called the order of G, and denoted by $ord(G)$. In that case G is called a finite group.

Remark: actually $(\mathbb{Z}/N\mathbb{Z})^\times$ with multiplication mod N is an Abelian group (make sure you understand it). Also note that the number of elements in this group is exactly Euler's ϕ function, i.e. $ord((\mathbb{Z}/N\mathbb{Z})^\times) = |(\mathbb{Z}/N\mathbb{Z})^\times| = \phi(N)$.

2. Subgroups

Definition: let G be a group (i.e. a set with a given map $* : G\times G \to G$ satisfying 1.1). A subset $H \subset G$ is called a subgroup of G if H is a group with respect to the restriction of the map $*$.

Easy fact: $1_G = 1_H$ (make sure you understand).

2.1. Lagrange's Theorem: let G be a finite group and H be a subgroup of G, then $ord(H)|ord(G)$.

The proof of this theorem is not difficult, but rather technical and requires the notation of co-sets (which is by itself quite technical). It may be found (for instance) in Wikipedia (both in English and in Hebrew) and requires no prior knowledge you do not have.

3. order of group elements

Notation: let $g \in G$ be a group element and let $n \in \mathbb{N}$, then $g^0 := 1_G$, $g^n := g*g*g*...*g$ (n times), and $g^{-n} := (g*g*g*...*g)^{-1}$ (n times).

3.1. Remark: let $g \in G$ be a group element. By definition $g^{-n} = (g^n)^{-1}$. Make sure you understand why also $g^{-n} = (g^{-1})^n$. Note that we obtained a notation that "behaves" like power laws in numbers, e.g. for all $a, b \in \mathbb{Z}$ we have $g^a * g^b = g^{a+b}, (g^a)^b = g^{ab}$.

3.2. Definition: let $g \in G$ be a group element. The minimal positive integer n such that $g^n = 1_G$ (if such n exists) is called the order of g, and denoted by $ord(g)$. In that case we say that g has finite order, or g is an element of order n. If such n does not exists we say that g has infinite order. Note that if g has finite order then $g^{-1} = g^{ord(g)-1}$.

3.3. Exercise: let G be a finite group and let $g \in G$. Prove that g has finite order and moreover that for any $n \in \mathbb{Z} : g^n = 1_G$ if and only if $ord(g)|n$. Hint: in order to show the first part consider all elements of the form $\{g^n\}_{n\in\mathbb{Z}} \subset G$. In order to show the second use division with remainder.

3.4. Exercise: let G be a group (not necessarily finite) and let $g \in G$. Denote $< g >:= \{g^n\}_{n\in\mathbb{Z}} \subset G$. Prove that $< g >$ is a subgroup of G.

Definition: a group of the form $< g >$ is called cyclic (i.e. a group G such that $\exists g \in G$ satisfying $G =< g >$). An element of a group satisfying $G =< g >$ is called a generator of G. Note that any cyclic group is Abelian and that if g is a generator then so is g^{-1}.

Example: $\mathbb{Z}$ with addition is an cyclic group with 1 and -1 being all possible generators.

3.5. Exercise: let G be a group (not necessarily finite) and let $g \in G$ be an element of finite order (see 3.2). Prove that $< g >$ is a finite group and that $ord(< g >) = ord(g)$.

Remark: by this exercise and Lagrange's Theorem we conclude that if G is a finite group then for any $g \in G$: $ord(g)|ord(G)$.

3.6. Exercise: (bonus) Prove Euler's Theorem: Let $N > 1$ be an integer and a be an integer which is co-prime to N, then: $a^{\phi(N)} \equiv 1 \ (mod\ N)$. Make sure you only use exercises and theorems we proved or quoted in this course (hint: using the relevant results this should be neither long nor difficult).

4. Homomorphisms and Isomorphisms

Definition: let G_1 be a group with a map $*_1$ and G_2 be a group with a map $*_2$. A map $\phi : G_1 \to G_2$ is called a group homomorphism if $\phi(1_{G_1}) = 1_{G_2}$ and for any $a, b \in G_1$: $\phi(a *_1 b) = \phi(a) *_2 \phi(b)$.

Definition: a group homomorphism is called a group isomorphism if it is one to one and onto.

Definition: we say that G is isomorphic to H if there exists a group isomorphism from G to H. In that case we write $G \cong H$.

4.1. Exercise: prove that isomorphism is an equivalence relation (hint: reflexivity is easy, for symmetry show that if $\phi : G \to H$ is a one to one and onto group homomorphism then so is $\phi^{-1} : H \to G$, and transitivity is shown by maps composition).

4.2. Example: let G be an Abelian group, and let H be a group such that $G \cong H$. Let us show that H is Abelian: let $h_1, h_2 \in H$. We need to show that $h_1 *_H h_2 = h_2 *_H h_1$. There exists a group isomorphism $\phi : G \to H$. It is surjective so there are $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Now using the properties of group homomorphism and the commutativity of G we get $h_1 *_H h_2 = \phi(g_1) *_H \phi(g_2) = \phi(g_1 *_G g_2) = \phi(g_2 *_G g_1) = \phi(g_2) *_H \phi(g_2) = h_2 *_H h_1$. □

4.3. Exercise: let G be a cyclic group, and let H be a group such that G is isomorphic to H. Prove that H is cyclic.

4.4. Exercise: let G be a group with $ord(G) = 36$, and assume it contains a unique subgroup G' such that $ord(G') = 9$. Let H be a group that is isomorphic to G. Prove that H contains a unique subgroup H' such that $ord(H') = 9$.

Important remark: 4.1-4.4 are examples of the general idea of category theory (here in the category of groups): two isomorphic objects are "the same" for all purposes in this category (e.g. two isomorphic groups are "the same" for all group related purposes). We want to stress the fact the this "being the same" property only holds inside the given category, e.g. two isomorphic groups are "the same" only as groups:

4.5. Exercise: prove that the set of integers divisible by 7 with the operation of addition (you showed in 1.2 that this is a group) is isomorphic to the group of integers with addition.

We "feel" that the set of integers divisible by 7 is not "the same" as the set of all integers in general, though they are "the same" (with addition) as groups. Next semester we will see that while the set of all integers is a Ring with a unit (a structure we will define), the set of all integers divisible by 7 is not.

The following exercise shows us that "being the same as sets" does not mean "being the same as groups":

4.6. Exercise: recall the fact that $\mathbb{Q}$ is countable, i.e. it is isomorphic to $\mathbb{Z}$ as sets. Both $\mathbb{Q}$ and $\mathbb{Z}$ are groups with the standard addition, and we saw that $\mathbb{Z}$ is cyclic. Prove that $\mathbb{Q}$ (with addition) is not cyclic. It follows from 4.3 that $\mathbb{Q}$ and $\mathbb{Z}$ are non-isomorphic groups, and we conclude that although $\mathbb{Q}$ and $\mathbb{Z}$ are "the same" as sets, they are "different" as groups.

The following exercise shows us that "being the same as groups" does not mean "being the same" in general, as $\mathbb{R}$ is a field, where $\mathbb{R}_{>0}$ is not:

4.7. Exercise: (bonus) Consider the group $\mathbb{R}$ with addition (real numbers with the operation of addition), and the group $\mathbb{R}_{>0}$ with multiplication (positive real numbers with the operation of multiplication). Check that both structures are indeed groups, and prove that they are isomorphic via the map $exp : \mathbb{R} \to \mathbb{R}_{>0}$ (i.e. $x \mapsto e^x$).

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