

MA-224 - WEEK 42
INTRODUCTION TO GROUP THEORY

SVERRE LUNØE-NIELSEN

CONTENTS

1. Introduction	1
2. Preliminaries on set theory	1
3. Definition	2
4. Examples	3
5. Homomorphisms and isomorphisms	6
6. Subgroups	7
7. Finite groups	7
8. Cyclic groups	8
9. Exercises	10
References	11

1. INTRODUCTION

In these notes we discuss topics from [2, §16.1-2]. During week 42, we aim to cover the essential parts of §3,4,6 and 8 during the lectures. In addition we include the definitions from §7, but we skip theorem 7.3.

We will postpone the topics of §5 until we get to coding theory in week 45 and 46.

2. PRELIMINARIES ON SET THEORY

If S is a set, we write $s \in S$ to indicate that s belongs to S . Given two sets S and T , the cartesian product $S \times T$ is the set consisting of all pairs (s, t) , where $s \in S$ and $t \in T$. In other words $S \times T = \{(s, t) \mid s \in S, t \in T\}$. A function of sets $f : R \rightarrow S$ is a rule which assigns for each $r \in R$ an element $f(r) \in S$. Two functions $f, g : R \rightarrow S$ are equal if $f(r) = g(r)$ for all $r \in R$. Two sets, R and S , are called isomorphic if there are functions $f : R \rightarrow S$ and $g : S \rightarrow R$ such that $g(f(r)) = r$ for every $r \in R$, and $f(g(s)) = s$ for every $s \in S$. If $\text{id}_R : R \rightarrow R$ is the identity function given by $\text{id}(r) = r$ for all $r \in R$, then we can summarize the above by saying that R and S are isomorphic if and only if there exists functions f and g such that $f \circ g = \text{id}_S$ and $g \circ f = \text{id}_R$.

Date: October 26, 2022.

3. DEFINITION

Let G be a set equipped with a closed binary operation, i.e. a function

$$(1) \quad \mu : G \times G \rightarrow G.$$

We say that (1) gives a way to multiply elements in G , and we often use the “in-fix”-notation

$$(2) \quad g \cdot h := \mu(g, h)$$

instead of referring to the function μ .

Definition 3.1. A **group** is a pair (G, \cdot) where G is a set and \cdot is a closed binary operation which satisfies the following rules:

- 1) For all elements $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. We say that the operation is associative.
- 2) There exists an element $e \in G$ such that $e \cdot a = a = a \cdot e$ for all $a \in G$. Such an element is called neutral.
- 3) For any element $a \in G$ there exists an element $b \in G$ such that $b \cdot a = e = a \cdot b$. Such an element is called inverse of a , and we often denote it by a^{-1} .

Remark 3.2 The first axiom tells us that we don’t need to keep track of parentheses when we compose elements using the group multiplication. Given $a, b, c \in G$, then there are two ways of multiply them together in that order: Either we do $a(bc)$ by first multiplying bc , followed by multiplication by a from the left, or we do $(ab)c$ by starting with ab and then multiplying by c from the right. Axiom 1 in the list above, however, says that these two ways of combining a, b, c produce the same result. Therefore, we usually drop the parentheses and simply write abc .

Remark 3.3 Let e and e' be neutral elements. Then $e = e \cdot e' = e'$, and so we conclude that $e = e'$. In other words: the neutral element is unique.

Remark 3.4 Any element $a \in G$ also has a unique inverse a^{-1} . The reason is that if b and c are both inverse to a , we get:

$$b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = e \cdot c = c.$$

Remark 3.5 If $e \in G$ is the neutral element in G , then e is its own inverse since $e \cdot e = e$ by the definition.

Remark 3.6 If $a, b \in G$, then

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$$

Therefore $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Definition 3.7. A group G is called **abelian** if $g \cdot h = h \cdot g$ for all elements $g, h \in G$.

4. EXAMPLES

Example 4.1 [The integers] Consider the set of natural numbers

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

We can combine elements of this set using normal addition of numbers, and this defines a closed binary operation. However, there is no neutral element, so this is not a group. We can fix this by adding 0 to the set. Then we have $0 + n = n$ for all natural numbers n , so 0 is the neutral element. But now the problem is that we have no inverses: Given $n > 0$, there are no other $m \geq 0$ such that $n + m = 0$. As we very well know, such an m must be a negative number. Therefore, it is not until we adjoin all the negative numbers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

we have a group. In fact, since $a + b = b + a$ for all integers a and b , the group of integers is abelian.

The letter \mathbb{Z} denoting the set of integers is rumoured to come from the first letter of the German word *Zahlen*, meaning “numbers”. Its use appears in print on page 20 of [1], but was used sporadically before as well.

Example 4.2 [The integers modulo n] Fix a natural number $n > 0$, and consider the relation between integers defined by $r \equiv t$ when $r - s$ is divisible by n . In other words, we say that $r \equiv s$ if there exists an integer k such that $r = s + kn$. It is easily checked that \equiv is an equivalence relation, and we denote by \mathbb{Z}/n the set of equivalence classes. Addition of integers induces a closed binary operation on \mathbb{Z}/n , which gives it the structure of an abelian group. We will check this claim.

If $r \in \mathbb{Z}$ is an integer, let $[r] \in \mathbb{Z}/n$ denote the equivalence class it belongs to. We defined $[r] + [s] = [r + s]$, and for this operation to be well defined, we need see that the result does not depend on the choice of representatives we make. In other words, we need to check that if $r' \equiv r$ and $s' \equiv s$, then $[r' + s'] = [r + s]$. There exist integers k, l such

that $r' = r + kn$ and $s' = s + ln$. Therefore, $r + s = r' + s' + n(k + l)$ which means that $r + s \equiv r' + s'$, so $[r + s] = [r' + s']$ just as we wanted.

Having established that our definition of the group operation makes sense, we need to check that it obeys the three group axioms of Definition 3.1:

The integer 0 gives rise to the neutral element $[0]$ since $[r] + [0] = [r + 0] = [r]$. Secondly, for any $[r] \in \mathbb{Z}/n$ we have $[r] + [-r] = [r - r] = [0]$, so the element $[-r]$ is an inverse.

Finally, associativity (axiom 1) in \mathbb{Z}/n follows from associativity in \mathbb{Z} : Given $r, s, t \in \mathbb{Z}$, then

$$\begin{aligned} [r] + ([s] + [t]) &= [r] + ([s + t]) \\ &= [r + (s + t)] \\ &= [(r + s) + t] = [r + s] + [t] \\ &= ([r] + [s]) + [t]. \end{aligned}$$

The group \mathbb{Z}/n is abelian since the group of integers is abelian: $[r] + [s] = [r + s] = [s + r] = [s] + [r]$.

Furthermore, since for every natural number k there exists a unique remainder $0 \leq k' < n$ such that $k \equiv k'$, the group \mathbb{Z}/n is finite and can be identified with the set

$$\mathbb{Z}/n = \{0, 1, 2, \dots, n - 1\}$$

of n remainders.

Example 4.3 We can make the set of real numbers into an abelian group by letting the closed binary operation be addition. We denote this group by $(\mathbb{R}, +)$.

Example 4.4 We can make the set of non-zero real numbers \mathbb{R}^\times into an abelian group by letting the closed binary operation be multiplication. We denote this group by $(\mathbb{R}^\times, \cdot)$. The reason we have to remove 0 from \mathbb{R} is that it has no inverse when the operation is multiplication.

Example 4.5 Let \mathbb{R} be the set of real numbers, and $M_n(\mathbb{R})$ the set of $n \times n$ -matrices with real entries. Then we can consider the sum of matrices in the usual way, which makes $M_n(\mathbb{R})$ an abelian group with neutral element the zero matrix.

Example 4.6 Let $GL_n(\mathbb{R})$ the set of invertible $n \times n$ -matrices with real valued entries. We turn this set into a group by letting the group

multiplication be matrix multiplication. Then $GL_n(\mathbb{R})$ becomes a non-abelian (why?) group with neutral element equal to the identity matrix.

Example 4.7 Let S be an alphabet of letters. The set of words which can be formed from S has a closed binary operation, with the empty word as neutral element. But just as in example 4.1, we lack inverse elements so this is not yet a group. To achieve this, we simply add letters to the alphabet which acts as inverses. Specifically, we form a new set $S^{-1} = \{s^{-1} \mid s \in S\}$, and then consider the alphabet which is the union of letters $S \cup S^{-1}$, from which we form words. For example, if $a, b, c \in S$, then words in our new alphabet can look like a^3cb^{-2} , or $b^{-1}c^2b^5$. Finally, we allow *reduction* of words: If two consecutive letters are inverse to each other, we remove them from the word. For example: $a^2b^{-1}bc^3 = a^2c^3$. When a word has reached its minimal length, it is called reduced. The set of *reduced* words form a group, where the operation is concatenation followed by reduction. The group of reduced words generated by the set S is called the *free group generated by S* .

Example 4.8 Let S_n be the set consisting of n elements $\{1, 2, 3, \dots, n\}$. A *permutation* of this set is a function $\sigma : S_n \rightarrow S_n$ which is bijection. We think of a permutation as a way of shuffling the elements of S_n . When we have two such shuffles, we can compose them and obtain a new shuffle. Precisely, if σ and η are two bijections $S_n \rightarrow S_n$, then the composite function $\sigma \circ \eta$ is yet again a bijection, i.e. a permutation of S_n .

The set of all permutations is denoted Σ_n and is a group by function composition. The neutral element is the identity function $S_n \rightarrow S_n$ sending k to k .

Example 4.9 Let A and B be groups. The cartesian product $G = A \times B$ becomes a group when endowed with the closed binary operation given by $(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$. The group $A \times B$ has neutral element (e_A, e_B) where e_A is the neutral element of A and e_B is the neutral element of B .

Example 4.10 Consider a regular n -gon P , for $n \geq 3$. Concretely, let P_n be the polygon with vertices equal to the set of the complex n -roots on unity: $\{e^{ik2\pi/n} \mid 0 \leq k < n\}$. A *symmetry* of P_n is a real linear transformation of the plane which preserves distances between points, and restricts to a permutation the vertices of P_n .

Two such linear transformations can be composed, and this gives the set of all symmetries, denoted D_n , the structure of a group.

To see that composition defines a closed binary operation, we first note that the composition of two distance-preserving linear transformations $g \circ f$ is again a distance-preserving linear transformation. Secondly, since both f and g acts on the vertices of P_n by a permutation, then the composition $g \circ f$ acts on the vertices by the composite permutation. Hence, $g \circ f$ is a linear transformation of the plane which permutes the vertices of P_n .

Any linear distance-preserving transformation T will have eigenvalues equal to ± 1 , since if v is an eigenvector associated with the eigenvalue λ , then $|\vec{v}| = |T(\vec{v})| = |\lambda \cdot \vec{v}| = |\lambda| \cdot |\vec{v}|$. Therefore, any symmetry has an inverse, and axiom (3) of 3.1 holds.

5. HOMOMORPHISMS AND ISOMORPHISMS

Given two groups, we compare them using the language of homomorphisms:

Definition 5.1. *Let G and H be groups. A **homomorphism** $\alpha : G \rightarrow H$ is a function of the underlying sets of G and H such that*

$$\alpha(g \cdot h) = \alpha(g) \cdot \alpha(h).$$

*A homomorphism α is an **isomorphism** there exists a homomorphism $\beta : H \rightarrow G$ such that $\alpha(\beta(h)) = h$ and $\beta(\alpha(g)) = g$ for all $g \in G$ and $h \in H$.*

We should think of homomorphisms as maps from one group to the other that preserve the group multiplication structures of the two groups.

The word stems from the Greek *homoios morphe* which means ‘similar form’.

Example 5.2 The real exponential function with base $a > 0$ is a group homomorphism from the real numbers under addition, to the group of positive real numbers under multiplication

$$\exp_a : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+, \cdot).$$

This is because of the familiar formula $\exp_a(x + y) = \exp_a(x) \cdot \exp_a(y)$. In fact, it is an isomorphism since its inverse, the base a -logarithm, is also a group homomorphism: $\log_a(x \cdot y) = \log_a(x) + \log_a(y)$.

Example 5.3 The determinant is a function from the group of invertible $n \times n$ -matrices to the non-zero real numbers under multiplication

$$\det : GL_n(\mathbb{R}) \rightarrow (\mathbb{R} \setminus \{0\}, \cdot).$$

This is because of the familiar formula $\det(M \cdot N) = \det(M) \cdot \det(N)$. It is an isomorphism if and only if $n = 1$.

6. SUBGROUPS

Definition 6.1. Let G be a group, and let $A \subset G$ be a subset which is not the empty set. We say that A is a **subgroup** G if:

- 1) $a \cdot b \in A$ for all $a, b \in A \subset G$. (Note that we use the binary operation in G , but demand that the result is contained in A .)
- 2) $a^{-1} \in A$ for all $a \in A \subset G$. (Again, we use the inverse as defined in the ambient group G but require that the result is contained in A .)

A subgroup $A \subset G$ is in itself a group. To see this, we must check the axioms 1-3. The first axiom is true since it is true in G . Axiom 3 holds per the definition above, so all that remains to check is that the neutral element $e \in G$ is also contained in A :

Since A is not empty, there exists an element $a \in A$. Because of axiom 2 in 6.1, the inverse a^{-1} is also in A . Because of axiom 1, the product will also be contained in A . But the product $a^{-1} \cdot a = e$ is the neutral element, so $e \in A$.

7. FINITE GROUPS

Definition 7.1. The order of a group G is the cardinality of its underlying set. The order of G is denoted by $|G|$.

Definition 7.2. Let G be a group. The order of an element g is the smallest natural number n such that $g^n = e$. If no such number exists, the order is said to be infinite. The order of g is denoted by $|g|$.

Theorem 7.3. Every finite group is a subgroup of a permutation group Σ_n , where $n = |G|$ is the order of G .

Proof. Enumerate the elements of $G = \{g_1, g_2, \dots, g_n\}$ from 1 to n . Any two element in the sequence $\sigma(g) := (gg_1 \ gg_2 \ \dots \ gg_n)$ are different. Also, every element gg_i is an element of G so it can be written as g_{i_j} for some index j unique to i . Therefore, $\sigma(g)$ can be thought of as a permutation of the elements of G , and we get function

$$\sigma : G \rightarrow \Sigma_n,$$

sending g to $\sigma(g)$.

We must show that this function is a group homomorphism. It is obvious that $\sigma(e)$ is the neutral element in Σ_n , and it follows from the associativity of the group multiplication that $\sigma(gh) = \sigma(g) \cdot \sigma(h)$ in Σ_n .

The cancellation property says that $g \cdot h = g' \cdot h$ implies that $g = g'$. This means that if $\sigma(g) = \sigma(h)$ as permutations, then $g = h$ as group elements of G .

In conclusion, we have shown that $\sigma : G \rightarrow \Sigma_n$ is an injective group homomorphism. So by Exercises 9.7 and 9.8, G is isomorphic to the image of σ , which is a subgroup of Σ_n . \square

8. CYCLIC GROUPS

Definition 8.1. A group G is **cyclic** if there exists an element $g \in G$ such that $G = \{g^k \mid k \in \mathbb{Z}\}$. We say that g is a generator for G , and write $G = \langle g \rangle$.

Example 8.2 The group of integers \mathbb{Z} is cyclic, and has exactly two generators: -1 and 1 . If $A \subset \mathbb{Z}$ is a subgroup, we let k be the smallest strictly positive integer which is contained in A . Then we claim that k generates A : If $n \in A$ and $n > 0$, we write $n = q \cdot k + r$ for $0 \leq r < k$. But then $n - q \cdot k = r$. Since n and $q \cdot k$ are both elements of A , $r \in A$. But $0 \leq r < k$, so $r = 0$ since k was the minimal strictly positive integer contained in A . Therefore $n = q \cdot k$. It follows that A is cyclic with generators $\pm k$.

This means that every subgroup of \mathbb{Z} is cyclic. In the remaining of this section we show similar statements for finite cyclic groups.

The following is immediate from the definitions:

Lemma 8.3. In a finite cyclic group G of order n , every generator has order n .

Example 8.4 For any n , the group \mathbb{Z}/n is cyclic with generator 1 .

Example 8.5 The group $\mathbb{Z}/6$ is cyclic, and it is generated by 1 and 5 . E.g. $\langle 5 \rangle = \{5, 4, 3, 2, 1, 0\}$ which are all the elements of $\mathbb{Z}/6$. Therefore, generators are not unique.

Lemma 8.6. Let $n > 1$. Then $\mathbb{Z}/n = \langle q \rangle$ if and only if $\gcd(q, n) = 1$.

Proof. Exercise 9.5. \square

Subgroups of cyclic groups are particularly simple:

Theorem 8.7. Let G be a finite cyclic group with generator g . If $A \subset G$ is a subgroup, then A is itself cyclic and its order divides $|G|$. In fact, $g^{|G|/|A|}$ generates A .

Proof. Since any element of G can be written as a power of g , so can any element of A . Let k be the minimal exponent such that $k > 0$ and $g^k \in A$. We will show that A is cyclic by showing that the element g^k generates A . In the process we will also discover that $k = |G|/|A|$.

Let $x \in A$ be any element. Again by the cyclicity of G there exists an exponent m such that $x = g^m$. Let $m = q \cdot k + r$ such that $0 \leq r < k$. Then $x = g^m = g^{q \cdot k + r} = g^{q \cdot k} \cdot g^r = (g^k)^q \cdot g^r$. It follows that $g^r = x \cdot (g^k)^{-q}$ is an element of A since A is a subgroup and x and $(g^k)^{-q}$ both belong to A . But $0 \leq r < k$ and k was assumed to be the minimal strictly positive integer such that $g^k \in A$. So this means that $r = 0$. Thus we have written $x = g^{q \cdot k} = (g^k)^q$ as a power of g^k . Since this argument holds for any element x it follows that the element g^k generates the entire subgroup A .

Since A is cyclic and g^k is a generator, this means that the order of g^k is $|A|$. In other words $(g^k)^{|A|} = e$, so

$$(3) \quad k \cdot |A| = q \cdot n$$

for some integer q . If $w = \gcd(q, |A|) \neq 1$, then $|A|/w$ is a natural number and $k \cdot |A|/w = q/w \cdot n$. This would mean that the order of g^k is less than $|A|$. Therefore, $w = 1$ which means that q must divide k and we get that $k' \cdot |A| = n$ where $k' = k/q$. Consider then the cyclic subgroup $A' = \langle g^{k'} \rangle$. Since $(g^{k'})^q = g^k$, it contains the cyclic subgroup A . On the other hand, $|A'| \leq n$ since $k' \cdot |A| \equiv 0 \pmod{n}$. But then

$$|A| \leq |A'| \leq |A|$$

so we must have $|A| = |A'|$. Since A is contained in A' as a subset, this means that $A = A'$. But then $g^{k'} \in A$ and $k' \leq k$ which means that $k' = k$ by the minimality of k . Finally, this means that $q = 1$ and (3) then reads $k \cdot |A| = n$ which means that $|A|$ divides $n = |G|$, and $g^k = g^{|G|/n}$ is a generator. \square

Lemma 8.8. *In a finite cyclic group of order n , the order of any element is a divisor of n .*

Proof. Let $g \in G$ be an element, and consider the subgroup $A = \langle g \rangle$. The order of g is equal to the order of A , which by Theorem 8.7 divides n . \square

Theorem 8.9. *Let $n > 0$ be a positive integer, and G a finite cyclic group of order n .*

Then any divisor d of n corresponds to a unique subgroup of G of order d , and if $A \subset G$ is a subgroup then $|A|$ is a divisor of n .

In other words, there is a 1-1 correspondence of sets

$$\{\text{subgroups of } G\} \leftrightarrow \{\text{divisors of } n\}.$$

Proof. Theorem 8.7 already says the $|A|$ is a divisor of n for every subgroup $A \subset G$. We need to show that this assignment is bijective.

Let $g \in G$ be a generator. Then to show surjectivity we note that any divisor d gives rise to a subgroup $\langle g^{n/d} \rangle \subset G$ which has order d .

Let A and B be (cyclic) subgroups of G of the same order m . Then if $g \in G$ is a generator of G , then Theorem 8.7 says that $A = B$ are the same subgroup since they are both generated by the same element $g^{n/m}$. \square

If G is a cyclic group with generator g , we can consider the function $f : \mathbb{Z} \rightarrow G$ which sends $k \mapsto g^k$ for every $k \in \mathbb{Z}$. Then $f(0)$ is the neutral element in G and $1 \in \mathbb{Z}$ is mapped to the generator $g \in G$. It is easy to see that f is a homomorphism of groups, since $f(m+n) = g^{m+n} = g^m \cdot g^n = f(m) \cdot f(n)$. It is also easy to check that f is surjective: Given any element $x \in G$, we write it as g^k for some power k of the generator g . But $g^k = f(k)$, so x is in the image of f .

In this sense, we can say that the group of integers is equal or larger than any other cyclic group we can think of.

Lemma 8.10. *Let G be a cyclic group of finite order $|G| = n$ and generator g . Then the homomorphism $f : \mathbb{Z}/n \rightarrow G$ defined by $f([k]) = g^k$ is an isomorphism.*

Proof. Let $[k] \in \mathbb{Z}/n$. The function f is well defined since the value $f([k])$ does not depend on the equivalence class representative for $[k]$. To see this, let q be any integer: Then $g^{k+qn} = g^k \cdot (g^n)^q = g^k \cdot 1^q = g^k$. Furthermore, f is a surjective homomorphism by the same reasoning as in the above discussion.

To show that it is an isomorphism, we construct an inverse homomorphism $f^{-1} : G \rightarrow \mathbb{Z}/n$ by the formula $f^{-1}(g^k) = [k]$. Be aware that given an element $x \in G$, then there are more than one way to write x as a power of the generator g . This is because $g^{r+n} = g^r$ for all integers r . However, if $g^t = e$, then $t = qn$ for some integer q . So if $g^r = g^s$ in G , then $e = g^s \cdot g^{-r} = g^{s-r}$ and so $r = s + qn$ for some integer q .

Therefore, f^{-1} is a well defined function, since the equivalence classes $[k]$ and $[k + qn]$ are equal in \mathbb{Z}/n .

It is easy to check that f^{-1} is a homomorphism and it is evident that $f(f^{-1}(g^k)) = g^k$ and $f^{-1}(f(k)) = k$. \square

9. EXERCISES

Exercise 9.1 Show that the free group generated by S is abelian if and only if $S = \{x\}$ is the singleton set.

Exercise 9.2 Show that Σ_2 is abelian. Then show that Σ_3 is not.

Exercise 9.3 Show that the abelian group $\mathbb{Z}/2 \times \mathbb{Z}/2$ is not cyclic.

Exercise 9.4 Show that the element 5 generate the group $\mathbb{Z}/6$, and then show that 2 or 3 do not.

Exercise 9.5 Show the following:

- (1) $\gcd(q, n) = n$ if and only if $q \equiv 0 \pmod{n}$.
- (2) $\gcd(q, n) = 1$ if and only if $kq \not\equiv 0 \pmod{n}$ for all $1 \leq k < n$.
- (3) $\mathbb{Z}/n = \langle q \rangle$ if and only if $kq \not\equiv 0$ for all $1 \leq k < n$.

Conclude, by (2) and (3), that $\mathbb{Z}/n = \langle q \rangle$ if and only if $\gcd(q, n) = 1$.

Exercise 9.6 Show that all cyclic groups are abelian.

Exercise 9.7 Show that the image of a homomorphism $f : G \rightarrow H$

$$\text{im}(f) = \{f(g) \mid g \in G\} \subset H$$

is a subgroup of H .

Exercise 9.8 Show that an injective homomorphism $f : G \rightarrow H$ defines an isomorphism $G \cong \text{im}(f)$.

Exercise 9.9 Show that a homomorphism $f : G \rightarrow H$ is an isomorphism if and only if f is a bijection as a function of sets.

Exercise 9.10 Show that a homomorphism $f : G \rightarrow H$ is an injection of sets if and only if $f(g) = e_H$ if and only if $g = e_G$.

Exercise 9.11 Let $O(n)$ be the subset of GL_n consisting of matrices of determinant equal to ± 1 . Show that $O(n) \subset GL_n$ is a subgroup.

REFERENCES

- [1] Nicolas Bourbaki, *Éléments de Mathématique. Algèbre. Chapitres 1 à 3*, Springer, 1970.
- [2] Ralph P. Grimaldi, *Discrete and combinatorial mathematics: an applied introduction.*, Pearson Education, 2013.

Email address: sverre.lunoe-nielsen@uia.no