

University of Delaware: Math 845. Fall 2011. F. Lazebnik.

The first four lectures are suggested as a review for Math 845, Fall 2011. All references to numbered Sections and Exercises are for D.S. Dummit and R.M. Foote “*Abstract Algebra*”, 3rd edition, John Wiley & Sons, Inc. These four lectures and suggested exercises are NOT mandatory, and can be easily replaced by introductory chapters to group theory from other undergraduate texts. Also in these notes you will see additional questions, some easy, some not-too-easy, and some very hard, often without indication of their difficulty. They are just to warm you up before the course, and to encourage you to learn to ask questions when you study a new topic.

Because the number of axioms for a group is very small, the variety of groups is very large. As fewer axioms define groups than other basic structures, like rings, fields, modules, algebras, some people get an impression that groups are easier to study compared to those structures. I do not think this is true. I often feel much more restricted in tools when I think about abstract groups compared to, say, fields. The notion of a group is fundamental. Groups provide a mathematical language to discuss symmetry, when it is understood in the broadest sense.

Mathematics is just a tale about groups.

– *H. Poincaré, 1881.*

Lecture 1. Review.

A **binary operation** ϕ on a set A is a function from $A \times A$ to A , i.e., $\phi : A \times A \rightarrow A$.

$\phi((x, y))$ is also denoted by $x\phi y$, or $x \cdot y$, or just xy .

A **group** (G, ϕ) is a non-empty set G with a binary operation ϕ , denoted $\phi(a, b) = ab$, which is

- (i) **Associative:** $(ab)c = a(bc)$ for all $a, b, c \in G$.
- (ii) There exists an **identity** element $e = e_G$ such that $ea = ae = a$ for all $a \in G$ (e “two sided”).
- (iii) For every $a \in G$, there exists $b \in G$ such that $ab = ba = e$. This element b is called an **inverse** of a in G , and is denoted by a^{-1} . (a^{-1} is “two sided”).

$|X|$ will denote cardinality of a set X . For a group G , $|G|$ is called **the order** of G . We write $|G| = \infty$, if G is infinite. G is **trivial** if $G = \{e\}$. G is **abelian** or **commutative** if $ab = ba$ for all $a, b \in G$. Often the operation in an abelian group is denoted by $+$, and we write $a + b$ instead of ab . In this case a^{-1} is denoted by $-a$.

FACTS: In any group G the following properties hold.

- (i) e_G is unique. Indeed, if e' is a possible another identity element, then $ee' = e$ as e' is an identity, and $ee' = e'$ as e is an identity. So $e = e'$.
- (ii) for each $a \in G$, the inverse of a is unique. Indeed, let b, b' be inverses of a . Then consider the element $(ba)b'$. Since $ba = e$, $(ba)b' = eb' = b'$. Similarly, consider $b(ab')$. Since $ab' = e$, $b(ab') = be = b$. Due to the associativity, $(ba)b' = b(ab')$. So $b' = b$.
- (iii) $(a^{-1})^{-1} = a$. Indeed, $aa^{-1} = a^{-1}a = e$ by definition of a^{-1} . Hence $a = (a^{-1})^{-1}$, again by definition of an inverse of a^{-1} .
- (iv) $(ab)^{-1} = b^{-1}a^{-1}$. Indeed, $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(e)a^{-1} = aa^{-1} = e$. Similarly, $(b^{-1}a^{-1})(ab) = e$. So $b^{-1}a^{-1}$ is the inverse of ab by the definition of the inverse.
- (v) Cancellation Law: in a group, $ab = ac$ or $ba = ca$ if and only if $b = c$.
To see it, just multiply both sides by a^{-1} from the left in the first case, and from the right – in the second.
- (vi) The product $a_1 \cdot a_2 \cdot \dots \cdot a_n$, $n \geq 3$, is understood as $((\dots (a_1 \cdot a_2) \cdot a_3) \dots) \cdot \dots \cdot a_n$, i.e., each time we apply it to two elements only. It can be shown to be independent on the way the factors are bracketed. For example, $abcd = ((ab)c)d = (ab)(cd) = (a(bc))d = a(b(cd))$. To show this, use induction on n .

By definition, for every $a \in G$, $a^0 := e$, $a^1 := a$, and for an integer $n \geq 2$, $a^n := aaa \dots a$, where we have n elements a and $(n - 1)$ multiplications. Define $a^{-n} := (a^n)^{-1}$. It is easy to check that the exponents behave as they should: $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$ for all $m, n \in \mathbb{Z}$.

H is a **subgroup** of a group $G = (G, \phi)$, denoted $H \leq G$, if $\emptyset \neq H \subseteq G$ and $(H, \phi|_H)$ is a group. Hence, the operation on H is the restriction of the operation of G on elements of H . It is easy to see that $e_G \in H$, and $e_H = e_G$. $\langle e \rangle$ and G itself are always subgroups of G . $\langle e \rangle$ is called the **trivial** subgroup. If $H \leq G$ and $H \neq G$, then H is called a **proper** subgroup of G . To stress that H is a proper subgroup of G , we write $H < G$.

Proposition 1. $H \leq G$ if and only if H is closed under the operation of G and under taking inverses. Moreover, if G is finite, $H \leq G$ if and only if H is closed under the operation of G .

If $H \leq G$, then $e_H = e_G$ and inverse of each $a \in H$ in H is the inverse of a in G .

Examples.

- Every ring (in particular, field) R is an abelian group under addition and the set of all units R^\times of ring R with 1 is a multiplicative group. In particular, if \mathbb{F} is a field, then $\mathbb{F}^\times = \mathbb{F} - \{0\}$ is an abelian group under multiplication. $n\mathbb{Z}$ is defined as $\{nz : z \in \mathbb{Z}\}$, and is a group under addition. Here is an example of two chains of groups. Groups in the first chain are under addition in \mathbb{C} , and in the second chain – under multiplication in \mathbb{C} .

$$n\mathbb{Z} < \mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C};$$

$$\mathbb{Z}^\times = \{1, -1\} < \mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times.$$

- Every vector space is an abelian group under addition.
- Let $GL(n, \mathbb{F})$ denote the group of all invertible $n \times n$ matrices over a field \mathbb{F} , or, equivalently, the group of all isomorphisms of an n -dimensional vector space over \mathbb{F} . It is called the **general linear group**. The operation is the matrix multiplication, or, composition of isomorphisms, respectively.
- $SL(n, R)$ – the group of $n \times n$ matrices over an integral domain R^1 with determinant 1. We have

$$SL(n, R) \leq GL(n, R).$$

- $S(X)$ – the group of all bijections of a set X to itself (the operation is composition of functions). It is called the **symmetric** group on X . Its elements are often referred to as **permutations** of X . For an infinite set X , the set of those bijections in $S(X)$ which move (i.e, do not fix) only finitely many elements of X form a subgroup in $S(X)$ denoted by $S^{fin}(X)$.
- $Isom(E^2)$ – the group of all distance preserving bijections (**isometries**) of points of the Euclidean plane E^2 .
- Let A be a nonempty subset of a group G and let

$$\langle A \rangle = \{a_1^{n_1} \cdot a_2^{n_2} \cdots a_k^{n_k} : \text{for all } k \in \mathbb{Z}, k \geq 1, \text{ all } a_i \in A, \text{ and all } n_i \in \mathbb{Z}\} =$$

$$\{a_1^{n_1} \cdot a_2^{n_2} \cdots a_k^{n_k} : \text{for all } k \in \mathbb{Z}, k \geq 1, \text{ all } a_i \in A, \text{ and all } n_i \in \{-1, 1\}\}.$$

Then $\langle A \rangle \leq G$. Moreover, $\langle A \rangle$ is the smallest (with respect to inclusion) subgroup of G containing A .

If $G = \langle A \rangle$, then it is said that A **generates** G . If $G = \langle A \rangle$ for a finite subset A , then G is called **finitely generated**. For $g \in G$, the subgroup $\langle \{g\} \rangle$, or simply $\langle g \rangle$, is called the **cyclic** subgroup generated by g . For $g \in G$, the order of $\langle g \rangle$, is called the **order of an element** g , and is denoted by $|g|$. Hence the order of an element of a group is the smallest positive integer n such that $g^n = e$, if such n exist. If it does not, we say that g has infinite order, and write $|g| = \infty$. If $G = \langle g \rangle$, group G is called **cyclic**, and g is called a **generator** of G .

¹If you do not know the definition of an integral domain, think about it as of \mathbb{Z} , or a field \mathbb{F} , or as the polynomial ring of one or more indeterminants with coefficients from \mathbb{Z} or \mathbb{F} .

If $G = \langle g \rangle$ is a finite cyclic group of order $n > 1$, then $G = \{g, g^2, \dots, g^{n-1}, g^n = e\}$, and all g^i , $1 \leq i \leq n$, are distinct. Also $g^a = g^r$ if and only if $a \equiv r \pmod{n}$. If G is an infinite cyclic group, then $G = \{g^n, n \in \mathbb{Z}\}$.

Theorem 1. Let $G = \langle g \rangle$, $n \in \mathbb{N}$, and $(a, n) = \gcd(a, n)$. Then

- (i) If $|g| = n$, then $|g^a| = |\langle g^a \rangle| = n/(a, n)$. Moreover, $G = \langle g^a \rangle$ if and only if $(a, n) = 1$. G has exactly $\phi(n)$ generators, where ϕ is the Euler's ϕ -function.
- (ii) If $|g| = \infty$, then g^a is a generator of G if and only if $a = \pm 1$.
- (iii) Every subgroup H of G is cyclic. H generated by g^a , where a is the smallest positive integer such that $g^a \in H$.
- (iv) If $|g| = n$, and $H = \langle g^a \rangle \leq G$, then a divides n . Conversely, for every positive divisor d of n , there is a unique subgroup of G of order d . This subgroup is generated by $g^{n/d}$.

Proof. Prove all statements of this theorem. (Students often underestimate the difficulty of giving a rigorous proof of this theorem.) \square

Given two groups G and H , a bijection $f : G \rightarrow H$ is called an **isomorphism** of G to H if for every $a, b \in G$, $f(ab) = f(a)f(b)$. If an isomorphism of G to H exists, group G is called **isomorphic** to H , and we write $G \cong H$. It is clear that isomorphism is an equivalence relation on the set of all groups, and an **abstract group** is just an equivalence class of this relation.

More examples of groups.

- We will often denote the (abstract) cyclic group of order n by C_n . The notation is justified as all cyclic group of order n are isomorphic. The infinite cyclic group is denoted by C_∞ . Clearly, $C_n \cong \mathbb{Z}/n\mathbb{Z}$, and $C_\infty \cong \mathbb{Z}$.
- Let Γ be a simple graph with $V = V(\Gamma)$ and $E = E(\Gamma)$ being its vertex set and edge set, respectively. The set of all bijections f of its vertex set V such that for all $x, y \in V$, $\{x, y\} \in E$ if and only if $\{f(x), f(y)\} \in E$, is a group (via composition of functions). It is called the **automorphism group of Γ** , and it is denoted by $\text{Aut}(\Gamma)$.
- Another important example is the the **dihedral** group D_{2n} , $n \geq 3$, of order $2n$. D_{2n} can be defined as the automorphism group of an n -cycle (i.e. a simple graph which is a cycle with n vertices and n edges). It can also be defined as the group of all distance preserving bijections (isometries) of the Euclidean plane which map a regular n -gon onto itself. Another way to define it is via generators and relations:

$$D_{2n} = \langle r, s \mid r^n = s^2 = e, rs = sr^{-1} \rangle.$$

This definition gives also such a description of all $2n$ elements of the group:

$$D_{2n} = \{e, r, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}.$$

Here r stands for a rotation by angle $2\pi/n$ around the center of the regular n -gon, and s is the symmetry of the n -gon with respect to a perpendicular bisector to one of its side. When we say that the same group can be defined in three ways, we, of course, mean that the three distinct groups defined these ways are all isomorphic (i.e. every two of them are isomorphic).

- If $G = H$, an isomorphism of G to G called an **automorphism** of G . It is easy to check that all automorphisms of G form a group with the operation being the composition of functions. This group is called the **automorphism group** of G , and it is denoted by $\text{Aut}(G)$.
- Given two groups G and H , one can consider the set

$$G \times H = \{(g, h) : g \in G, h \in H\},$$

with the operation on $G \times H$ defined as follows: $(g, h) \cdot (g', h') = (gg', hh')$, where the operation on the first coordinate is the one of G , and on the second – of H . Then $G \times H$ with this operation is a group, called the (external) **direct product** of G and H . Clearly, the subgroup of $G \times H$ formed by all pairs (g, e_H) is isomorphic to G , and the subgroup formed by all pairs (e_G, h) is isomorphic to H . Clearly the direct product of groups can also be considered as **an operation** on the set of all groups. The result of this operation applied to groups G and H is $G \times H$.

Despite the simplicity of the definition, the structure of group $G \times H$ is not too simple. It is clear that if $G_1 \leq G$ and $H_1 \leq H$, then $G_1 \times H_1 \leq G \times H$. But not every subgroup of $G \times H$ is formed this way. Consider, e.g., $D = \{(x, x) : x \in G\}$, called the **diagonal subgroup** of $G \times G$. Then $D \leq G \times G$, but it is not the direct product of two subgroups of G if $|G| \geq 2$.

It turns out that a few examples of groups we have presented, together with the operation of direct product of groups, allows to describe large classes of groups. For example, an important theorem that we will prove states that every finitely generated abelian group is isomorphic to a direct product of finitely many cyclic groups.

The examples above illustrate that some groups, e.g., $S(X)$, $\text{Aut}(\Gamma)$, $\text{Aut}(G)$, D_{2n} , $GL(n, \mathbb{F})$ appear as the sets of symmetries of a mathematical object. It is often said that the language of groups is the language for the study of SYMMETRY in mathematics and the world. but what is symmetry? Symmetries of what object are described by $SL(n, \mathbb{Z})$?

Questions

One fool can ask ten times more questions than ten wise people.

– *Russian proverb*

Some of these questions may be hard, but they seem natural at this point.

- How many abstract groups of order n are there?
- Can a group G of order n have no subgroups apart $\langle e \rangle$ and G ? Can an infinite group have this property?
- Is every infinite group finitely generated? Can a group be generated by its five elements, but not by four elements? Does the answer depend on whether the group is finite?
- How many elements generate C_{2010} ? And how many subgroups does it have?
- Is there a nonabelian finite group G whose all proper subgroups are abelian? Whose all proper subgroups are cyclic? Does an answer change if G is infinite?
- Can an infinite group have only finitely many subgroups?

(vii) Can an infinite group have each of its proper non-trivial subgroup finite?

Assignment 1.

Read these notes and Sections 1.1, 1.2, 1.4, 1.5, 1.6. 2.1, 2.3. 2.4 from the text. Some of the material in these chapters will be briefly discussed in class next time.

Problems. Most of the problems below is a review of what many students have seen/studied.

Section 1.1: 7, 14 – 36 .

Section 1.2: 7, 18.

Section 1.4: Prove the statements at the end of Section 1.4, namely that the number of element in any finite field is a power of a prime, and that $|GL(n, F_q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$. Do also #11.

Section 1.5: 1 – 3.

Section 1.6: 4 – 9, 11, 17 – 19, 24 – 26.

Section 2.1: 4, 6, 8 – 11, 14 – 17.

Section 2.3: 1, 2, 4, 10 – 13, 15 – 17, 21 – 23 (these facts are used in the complete description of the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$), 26.

Section 2.4: 1, 2, 4, 13 – 16, 18 (a great example: an infinite group with every subgroup finite and cyclic, hence generated by one element, but the whole group is not finitely generated) 19 – 20 (the structure of divisible groups is well understood. It allows to prove, e.g., the following amazing fact: two multiplicative groups \mathbb{C}^\times and $U = \{z \in \mathbb{C} : |z| = 1\}$ are isomorphic.)

Section 2.5: 3, 12, 13.

- (i) What are the elements of \mathbb{C}^\times of order n ? Of any finite order? Show that all elements of finite order in \mathbb{C}^\times form a subgroup. Can you describe this subgroup in terms of familiar groups?

Show that $z = e^{i\alpha}$, where $\alpha = \cos^{-1}(1/3)$, has infinite order in \mathbb{C}^\times .

- (ii) An **elementary matrix** is an n by n matrix of the form $I + cE_{ij}$, where $I = I_n$ is the identity n by n matrix, $i \neq j$, $c \neq 0$, and $E_{i,j}$ has 1 in (i, j) -position and 0's everywhere else. Show that $GL(n, \mathbb{F})$ is generated by elementary matrices.

- (iii) Show that group $SL(2, \mathbb{Z})$ is generated by the matrices

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Lecture 2. Review.

It is clear that for all n -element sets X , the symmetric groups $S(X)$ are isomorphic. By S_n we will denote the corresponding abstract group. Often we use $[n] = \{1, 2, \dots, n\}$ for X and assume that $S_n = S([n])$. The elements of S_n are called **permutations** of the set $[n]$, or **n -permutations**. It is clear that $|S_n| = 1 \cdot 2 \cdot 3 \cdots n = n!$. If $\pi, \sigma \in S_n$, then $\tau = \pi\sigma = \pi \circ \sigma$ is an element of S_n defined as $\tau(x) = \pi(\sigma(x))$. Hence the “product of π and σ ” is the composition of σ (applied first) and π .

In enumerative combinatorics r -permutations are often thought and represented as ordered r -tuples of distinct elements of an n -element set, $r \leq n$. In group theory, we think about the permutations as elements of a group, and the dominating way of representing them is as the **product of disjoint cycles** or the **cycle decomposition**. Let $2 \leq k \leq n$ and a_1, \dots, a_k be distinct elements of $[n]$. A **k -cycle** $c = (a_1 a_2 \dots a_k)$ in S_n , $2 \leq k \leq n$, is a bijection of $[n] \rightarrow [n]$ defined as: $c(x) = x$ if $x \notin \{a_1, a_2, \dots, a_k\}$, $c(a_i) = a_{i+1}$ for all $1 \leq i \leq k-1$, and $c(a_k) = a_1$. A k -cycle is also called a **cycle of length k** . A 2-cycle is called a **transposition**. A 1-cycle (a) can be defined as the identity map on $[n]$. In this case all (a) represent the same (identity) permutation for every $a \in [n]$. If $\pi(a) = a$, then a is called a **fixed point** of π .

For example, a bijection $\pi : [7] \rightarrow [7]$ given by

$$1 \mapsto 3, \quad 2 \mapsto 2 \text{ (fixed)}, \quad 3 \mapsto 4, \quad 4 \mapsto 1, \quad 5 \mapsto 7, \quad 6 \mapsto 6 \text{ (fixed)}, \quad 7 \mapsto 5,$$

can be written briefly as $\pi \in S_7$ as $\pi = (134)(57)$, or $(341)(57)$, or $(341)(75)$, or $(134)(2)(57)(6)$. In the last representation, the fixed points are shown explicitly. Also, the same π can be thought as a *product* of two permutations in S_7 , which are the 3-cycle (134) and the transposition (57) . Clearly representations which differ only by listing of fixed points or by changing the order inside parenthesis “cyclically” describe the same bijection.

Why can we represent any $\pi \in S_n$ as a product of cycles which share no common elements?

Note that a binary relation \sim on $[n]$, defined as $x \sim y$ if and only if there exists an integer i such that $\pi^i(x) = y$, is an equivalence relation. The corresponding equivalence classes, called sometimes **orbits of π** (or of $\langle \pi \rangle$), are disjoint and elements in each class can be ordered as $a, \pi(a), \pi^2(a), \dots, \pi^{k-1}(a)$, for some $k \geq 1$ which usually depends on a . This gives the cycles in the **cycle decomposition of π** , i.e., in any representation of π as a product of cycles such that distinct cycles share no common elements. The corresponding uniqueness statement follows by induction on n . The uniqueness is understood up to the order of cycles. Remember that disjoint cycles commute.

We say that two permutation in S_n have **same type cycle decompositions** if there exists a bijection between the sets of cycles in the their cycle decompositions which preserves the length of cycles. For example, $\pi = (1345)(79)$ and $\sigma = (45)(1236)$ of S_{12} have same type cycle decomposition, since each has one 4-cycle, one transposition and six fixed points (“1-cycles”).

The following useful fact relates the property of two permutations having same type cycle decomposition to a group-theoretic property of conjugacy in G . Elements a and b in a group G are called **conjugate** if $b = xax^{-1}$ for some $x \in G$.

Theorem 2. Let $\tau, \sigma \in S_n$ and

$$\sigma = (a_1 \dots a_{k_1})(b_1 \dots b_{k_2}) \dots$$

be the cycle decomposition of σ . Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$\tau\sigma\tau^{-1} = (\tau(a_1) \dots \tau(a_{k_1}))(\tau(b_1) \dots \tau(b_{k_2})) \dots$$

Conversely, if two permutation in S_n have same type cycle decompositions, then they are conjugate.

Proof. If $\sigma(i) = j$, then $\tau\sigma\tau^{-1}(\tau(i)) = \tau(j)$. In other words, if i and j are subsequent elements of a cycle of σ , then $\tau(i)$ and $\tau(j)$ are subsequent elements of a cycle of $\tau\sigma\tau^{-1}$. Hence conjugate permutations have same type cycle decomposition.

Conversely, let $\sigma = (a_1 \dots a_{k_1})(b_1 \dots b_{k_2}) \dots$ and $\gamma = (c_1 \dots c_{k_1})(d_1 \dots d_{k_2}) \dots$ be two permutation of same cycle type. Then $\delta : [n] \rightarrow [n]$ defined as $\delta(a_i) = c_i$ for all $i = 1 \dots, k_1$, $\delta(b_j) = d_j$ for all $j = 1 \dots, k_2$, etc., is a permutation on $[n]$, and $\delta\sigma\delta^{-1} = \gamma$. \square

Questions

Some of these questions may be hard, but they seem natural at this point.

- (i) We say that $\pi \in S_n$ has the **cycle decomposition of type** $t = (k_1, k_2, \dots, k_n)$, or just **type** $t = (k_1, k_2, \dots, k_n)$ if the cycle decomposition of π has exactly k_i cycles of length i , $i \in [n]$. For example, $\pi = (134)(57)$ of S_7 has type $(2, 1, 1, 0, 0, 0, 0)$, and $\sigma = (45)(1236)$ of S_{12} has type $(6, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$. How many permutations in S_n have type t ?
- (ii) How many permutations of S_n have exactly k cycles in their cycle decomposition if 1-cycles are allowed? What if 1-cycles are not allowed?
- (iii) What is the average number of cycles in the cycle decompositions of all elements of S_n ?
- (iv) How many permutations of S_n have exactly k fixed points, $0 \leq k \leq n$? What is the average number of fixed points of all elements of S_n ?
- (v) How many distinct types of cycle decompositions of elements of S_n are there?
- (vi) What is the order of a random element of S_n ? In other words, if each elements of S_n is chosen with probability $(n!)^{-1}$, what is the expected value of its order?

The following theorem describes several important properties of cycles in S_n .

Theorem 3. (i) *The order of a permutation is the l.c.m of the cycles length in its cycle decomposition.*

- (ii) *The number of m -cycles in S_n , $1 \leq m \leq n$, is $n(n-1)(n-2) \dots (n-m+1)/m$.*
- (iii) *$(a_1 a_2 \dots a_k) = (a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_2)$, i.e., every k -cycle, $k \geq 2$, is a product of $k-1$ transpositions.*
- (iv) *Every element of S_n , $n \geq 2$, can be written as a product of transpositions, and the parity of the number of transpositions does not depend on the representation. A permutation which is a product of an even (odd) number of transpositions is called **even permutation** (**odd permutation**).*

- (v) The set of all even permutations of S_n form a group, called the **alternating group of degree n** , and denoted by A_n . $A_1 = S_1$. For $n \geq 2$, the order of A_n is $n!/2$.
- (vi) S_n can be generated by two cycles. For example,

$$S_n = \langle (12), (123 \dots n) \rangle$$

(which means the same as $\langle \{(12), (123 \dots n)\} \rangle$).

S_n can be generated by some sets of its $n - 1$ transpositions, like

$$S_n = \langle (12), (13), \dots, (1n) \rangle,$$

or by adjacent transpositions:

$$S_n = \langle \{(i \ i + 1), i \in [n - 1]\} \rangle = \langle (12), (23), (34), \dots, ((n - 1) n) \rangle.$$

S_n cannot be generated by any set of less than $n - 1$ transpositions.

Proof. (i) Disjoint cycles commute. If $\pi = c_1 c_2 \dots c_k$ is the cycle decomposition of π , and $d = |\pi|$, then $e = \pi^d = c_1^d c_2^d \dots c_k^d$. Next, $\pi^d = e$ if and only if $c_i^d = e$ for all $i \in [k]$. The latter is equivalent to $|c_i|$ divides d for all i . Then $d = \text{l.c.m}(|c_1|, |c_2|, \dots, |c_k|)$, since d is the smallest integer divisible by all $|c_i|$.

(ii) There are $n(n - 1)(n - 2) \dots (n - m + 1)$ way of choosing m elements for an m -cycle and ordering them. Exactly m of these ordered m -tuples will represent the same cycle. The result follows.

(Remark: if one wants to count the number of m -cycles in a complete graph K_n (here an m -cycle is meant as a *subgraph* of K_n), the answer will be twice smaller due to m reflections in its automorphism group, i.e., it will be $n(n - 1)(n - 2) \dots (n - m + 1)/(2m)$.)

(iii) Just notice that both $(a_1 a_2 \dots a_k)$ and $(a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_2)$ map a_i to a_{i+1} for $i \in [k - 1]$, map a_k to a_1 , and fix all other elements.

Writing every cycle in the cycle decomposition of an element $\pi \in S_n$ as a product of transpositions, we obtain its representation as a product of transpositions. (Such representation is usually not the cycle decomposition of π as different transpositions may share common elements of $[n]$.)

(iv) The statement concerning the parity of the numbers of transpositions in different representations of the same permutation as a product of transpositions is *not(!!!)* obvious. It is clearly equivalent to the statement that the identity permutation is always a product of an even number of transpositions. To prove the latter, we will use the following lemma.

Lemma 1. *Let $\pi \in S_n$ and let τ be a transposition in S_n . Then the number of cycles in the cycle decomposition of π and the cycle decomposition of $\tau\pi$ differs by one.*

Proof. Do it. □

Let now $e = \tau_1 \tau_2 \dots \tau_k$, where all τ_i are transpositions. Then $e = \tau_1 \tau_2 \dots \tau_k e$. According to the lemma above, we alter the number of cycles of e , which is zero, by one exactly k times. Since at the end the number of cycles is zero again, k must be even.

(v) Clearly the set of even permutations in S_n is closed under the multiplication. It is also closed under taking inverses, since for arbitrary transpositions τ_i ,

$$(\tau_1 \tau_2 \dots \tau_k)^{-1} = \tau_k^{-1} \dots \tau_2^{-1} \tau_1^{-1} = \tau_k \dots \tau_2 \tau_1.$$

Hence A_n is a group. Fix a transposition τ . For any odd permutation σ , $\tau\sigma \in A_n$. Hence $\sigma \in \tau^{-1}A_n = \tau A_n$. As elements of τA_n are all distinct odd permutations, and $|A_n| = |\tau A_n|$, we have $|A_n| = |S_n|/2 = n!/2$.

(vi) As all transpositions generate S_n , it is sufficient to show that, in each case, an arbitrary transposition can be written by using the generators. Let $n \geq 3$ and $1 \leq i < j \leq n$. We have

$$\begin{aligned}(ij) &= (i \ i+1) (i+1 \ i+2) \cdots (j-1 \ j) (j-1 \ j-2) \cdots (i+1 \ i) \\(i+1 \ i+2) &= (12 \dots n)^i (12) (12 \dots n)^{-i}, \text{ for } i \in [n-2] \\(12 \dots n) &= (12) (13) (14) \cdots (1n).\end{aligned}$$

The first line shows that $\{(i \ i+1)\}$, $i \in [n-1]$, generates all transpositions, and hence the whole S_n . The second relations show that $\{(12), (12 \dots n)\}$ generate all adjacent transpositions $\{(i \ i+1)\}$, $i \in [n-1]$. So they also generate S_n . The third relation show that $\{(12), (13), \dots, (1n)\}$ generate the n -cycle $(12 \dots n)$, and hence the whole S_n . Another way to show that $\{(12), (13), \dots, (1n)\}$ generate S_n to generate all (ij) first:

$$(ij) = (1i)(1j)(1i).$$

A proof of the statement that less than $n-1$ transpositions never generate S_n is left to the reader. \square

Questions

Some of these questions may be hard, but they seem natural at this point.

- (i) Prove that it is impossible to generate S_n , $n \geq 2$, with less than $n-1$ transpositions.
- (ii) How many different sets of $n-1$ transpositions generate S_n ?
- (iii) Can any group of order $n \geq 2$ be generated by its two elements?
- (iv) Is any finite group a subgroup of another finite group which is generated by two elements?
- (v) What is the average cardinality of a generating set of S_n ? Of a minimal generating set of S_n ? What is the expected order of a subgroup of S_n generated by a random k -subset of its elements? Here we assume that all k -element subsets are chosen with the same probability $\binom{n}{k}^{-1}$.

Assignment 2.

Read these notes and Section 1.3.

Problems. Most of the problems below is a review of what many students have seen/studied.

Section 1.3: 9 – 20.

- (i) Prove that the order of any element of S_n does not exceed $e^{n/e} \approx 1.44^n$. How close to this upper bound can you get?

Lecture 3. Review.

Given group G and its subgroup H one can try to build a new group in a way the ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ was built from \mathbb{Z} .

The latter was done along these lines: an equivalence relation, namely congruence modulo n , was introduced on \mathbb{Z} . One way to define the congruence is to say that $a \equiv b \pmod{n}$ if $a - b \in n\mathbb{Z}$. Note that $n\mathbb{Z} \leq \mathbb{Z}$, and every subgroup of \mathbb{Z} is of such form. The congruence relation turned out to be an equivalence relation on \mathbb{Z} . Then the operations on equivalence classes were defined by using representatives of the classes, with preliminary verification that it did not matter which representative from a class is chosen for this purpose. Then it was easy to check that \mathbb{Z}_n is a commutative ring with n elements.

Let's try to imitate this construction for an arbitrary group G and its subgroup H . Consider a binary relation \sim on G defined as: $a \sim b$ if $ab^{-1} \in H$. It is easy to check that \sim is an equivalence relation, and, for $x \in G$, the equivalence class $[x] := \{y : y \sim x\}$ is precisely $Hx := \{hx : h \in H\}$. The set Hx is called the **right cosets** of H in G , and we denote the set of all right cosets by $(G : H)$. (The same notation will be used for the set of the **left** cosets xH , which are defined similarly.) The coset Hx is the equivalence class containing x . Trying to define an operation on the set of all cosets by using the same idea as for \mathbb{Z}_n , namely, $Hx \cdot Hy := H(xy)$, we first have to check that such operation is well-defined, i.e., does not depend on our choice of the representatives from the cosets. More precisely, the question we have to resolve is the following: is it true that for any $x_1, x_2 \in Hx$ and any $y_1, y_2 \in Hy$, the products x_1y_1 and x_2y_2 belong to the same coset? Or, equivalently, is it true that if $x_1x_2^{-1} \in H$ and $y_1y_2^{-1} \in H$, then $(x_1y_1)(x_2y_2)^{-1} = (x_1y_1)(y_2^{-1}x_2^{-1}) \in H$?

Suppose we wish to prove that the answer to the question is always 'Yes'. We will experience the difficulties. Analyzing the success we had with \mathbb{Z}_n , we conclude that it was due to commutativity of the addition in \mathbb{Z} . Can this be 'fixed' for non-abelian groups? The example below shows that, in general, the answer is 'No'.

Example. Let $G = S_3$ and $H = \langle (12) \rangle$. There are three right cosets of H in G :

$$H = \{e, (12)\}, \quad H(13) = \{(13), (132)\}, \quad H(23) = \{(23), (123)\}.$$

Then take $x_1 = (13)$, $x_2 = (132)$ from $H(13)$, and $y_1 = (23)$, $y_2 = (123)$ from $H(23)$.

Then

$$(x_1y_1)(y_2^{-1}x_2^{-1}) = (12)(23)(132)(123) = (123) \notin H.$$

So, when does $\{Hx : x \in G\}$ form a group under the operation $(Hx)(Hy) = H(xy)$? This question leads to the definition of a normal subgroup of G .

A subgroup H of G is called **normal** if for every $x \in G$, $xH = Hx$. The condition $xH = Hx$ is equivalent to $xHx^{-1} = H$ or to $x^{-1}Hx = H$. If H is normal subgroup in G , we write $H \trianglelefteq G$. If H is a proper normal subgroup, we will write $H \triangleleft G$.

For every $H \leq G$, one can consider the largest (in terms of inclusion) subgroup K of G such that $H \trianglelefteq K$. Such clearly exists, since $H \trianglelefteq H$. It is called the **normalizer** of H in G and is denoted by $N_G(H)$. So we have: for every subgroup H of G , $H \trianglelefteq N_G(H)$. Clearly, $H \trianglelefteq G$ is equivalent to $N_G(H) = G$.

We collect several results related to the notions of a coset and normality in the following theorem, and leave the proofs to the reader.

Theorem 4.

- (i) $H \trianglelefteq G$ if and only if the operation on the right cosets $HxHy = H(xy)$ makes $(G : H)$ a group. Similar statement holds for the left cosets with operation $xHyH = (xy)H$.
- (ii) If $N \trianglelefteq G$ and $H \leq G$, then $N \cap H \trianglelefteq G$. Intersection of any collection of subgroups of G having a normal subgroup among them is a normal subgroup of G .
- (iii) If $A \leq B \leq G$ and $A \trianglelefteq G$, then $A \trianglelefteq B$.
- (iv) $N_G(H) = \{g \in G : gH = Hg\}$.
- (v) If $A \trianglelefteq B \trianglelefteq G$, then A is not necessarily normal in G .

The group described in Theorem 4 ((i)) is called the **factor group** of G with respect to H , and is denoted by G/H .

Before we move further, we wish to state a very important result which immediately follows from our studies and is NOT connected to the notion of normality. By $|G : H|$ we denote the cardinality of the set $(G : H)$. It is called the **index** of H in G .

Since the equivalence classes partition G and all have the same number of elements, we have

Theorem 5. (Lagrange's Theorem) *If G is a finite group and $H \leq G$, then*

$$|G| = |H||G : H|,$$

and so both the order and the index of H divide the order of G .

The following corollary immediately follows. It gives, in particular, another proof of the result we obtained before for cyclic group.

Corollary 1. *The order of an element of a finite group divides the order of the group.*

The converse of Lagrange theorem, in the sense that for every divisor d of $|G|$ there exists a subgroup of G of order d , is, generally, false. For example, it is easy to show that A_4 , which has order 12, has no subgroup of order 6.

It is known that the result (the converse of Lagrange theorem) holds for finite abelian groups, or for all divisors of $|G|$ which are prime powers. These remarkable facts are not easy to prove. We will do it later in the course.

A generalization of Lagrange's theorem is the following

Theorem 6. *If $A \leq B \leq G$ and both $|B : A|$ and $|G : B|$ are finite, then*

$$|G : A| = |G : B||B : A|.$$

Lagrange theorem follows from Theorem 6 if A is the trivial subgroup.

The notion of a normal subgroup also appears when we try to answer this question:

What is the smallest subgroup which contains given two subgroups A and B of a group G ?

By analogy with vector spaces, or modules or fields, one candidate is

$$AB := \{ab : a \in A, \text{ and } b \in B\}.$$

An attempt to prove it for abelian groups succeeds, but it fails if G is not abelian. On the other hand, the proof is easy if one of the group is normal in G . Analyzing a little more we get the following result:

Theorem 7. *Let $A, B \leq G$ and $A \trianglelefteq G$ or $B \trianglelefteq G$. Then $AB \leq G$. Moreover, the conclusion $AB \leq G$ holds under a weaker condition: $A \leq N_G(B)$ or $B \leq N_G(A)$.*

To finish with AB , we wish to present another interesting and useful fact which holds even if AB is not a subgroup.

Theorem 8. *Let G be a finite group, and let $A \leq G$ and $B \leq G$. Then*

$$|AB| = \frac{|A||B|}{|A \cap B|}.$$

Questions

Some of these questions may be hard, but they seem natural at this time.

- (i) Suppose H is not normal in G .
 - (i) Can a left coset different from H coincide with a right coset different from H ?
 - (ii) If $|G : H|$ is finite, can the set of all left cosets coincide with the set of all right cosets? The answer is affirmative (see part (iii)). Show that if $|G : H| = 2$, this necessarily happens. Give an example of H and G , $|G : H| = 3$, with distinct collections of all right and all left cosets.
 - (iii) Let G be a finite group, $H \leq G$, H is not normal in G , and $|G : H| = n$. It turns out that it is always possible to find $x_1, \dots, x_n \in G$, such that $\{x_i H : i = 1, \dots, n\}$ is the set of all left cosets and $\{H x_i : i = 1, \dots, n\}$ is the set of all right cosets. This is a corollary from a famous combinatorial theorem by P. Hall ('The Marriage Theorem').
- (ii) Let $H \leq G$. Can both H and $(G : H)$ be infinite? For a given positive integer n , can we always find a group G and its subgroup H such that $|G : H| = n$?
- (iii) If $A, B \leq G$ of finite indices, will $|G : A \cap B| = |G : A||G : B|$?
- (iv) Give an example of a non-abelian group G without a proper nontrivial normal subgroup H .

Assignment 3.

Read Section 3.1 – 3.2 or any shorter version of this material in your favorite place.

Problems:

Sec. 3.1: 3, 5, 9, 12, 14, 15, 22, 35 – 41.

Sec. 3.2: 5, 8, 11, 16 – 22.

Lecture 4. Review.

Another natural way one can arrive to the notion of a normal subgroup is via studying group homomorphisms.

Let G and H be two group and $\phi : G \rightarrow H$ such that $\phi(ab) = \phi(a)\phi(b)$ for every $a, b \in G$. Such a function is called a **homomorphism** from G to H . When ϕ is bijective, we get that ϕ is a group isomorphism, the notion which has been already introduced. It turns out that $\phi^{-1}(e_H)$ is always a (non-empty) subgroup of G , called the **kernel** of ϕ , and denoted $\ker \phi$. Moreover, it turns out that the subgroup $\ker \phi$ necessarily has the property that $g(\ker \phi) = (\ker \phi)g$!

Group homomorphism are analogs of linear mapping of vector spaces. The definition for groups is even simpler. Paraphrasing one group theory text, the homomorphic image $\phi(G)$ is an identification of one person (sometimes a very blurred document) in the pocket of another.

Here we collect some properties of group homomorphisms. Every one has to check them at least once in their lives. Why not now?

Theorem 9. *Let $\phi : G \rightarrow H$ be a group homomorphism.*

- (i) $\phi(e_G) = e_H$, $\phi(g^{-1}) = (\phi(g))^{-1}$ for every $g \in G$, and $\phi(G) \leq H$.
- (ii) $\ker \phi \trianglelefteq G$.
- (iii) If $G_1 \leq G_2 \leq G$, then $\phi(G_1) \leq \phi(G_2) \leq \phi(G)$.
If $G_1 \trianglelefteq G_2 \leq G$, then $\phi(G_1) \trianglelefteq \phi(G_2) \leq \phi(G)$.
- (iv) If ϕ is surjective, then $\phi^{-1}(H) \leq G$. Moreover, if
 - (i) $H_1 \leq H_2 \leq H$, then $\phi^{-1}(H_1) \leq \phi^{-1}(H_2) \leq \phi^{-1}(H)$.
 - (ii) $H_1 \trianglelefteq H_2 \leq H$, then $\phi^{-1}(H_1) \trianglelefteq \phi^{-1}(H_2) \leq \phi^{-1}(H)$.

The following four statements are known as **The Isomorphism Theorems (IT)**. They are very useful tools in group theory.

Theorem 10.

- (i) *(The First IT)* If $\phi : G \rightarrow H$ is a group homomorphisms, then $G/\ker \phi \simeq \phi(G)$
- (ii) *(The Second IT)* Let A and B be subgroups of G and $A \leq N_G(B)$. Then $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \simeq A/A \cap B$.
- (iii) *(The Third IT)* Let A and B be normal subgroups of G , and let $A \leq B$ (hence $A \trianglelefteq B$). Then $B/A \trianglelefteq G/A$ and $G/A \simeq (G/B)/(B/A)$.
- (iv) *(The Fourth IT)* Let $A \trianglelefteq G$. There is a bijection between the set of subgroups of G which contain A and the set of subgroups of G/A .

Proofs of the results presented in this lecture are not hard and the reader is encouraged to complete them by her/himself. In case of difficulties, see the recommended texts.

The First IT implies that if one wants to know what are all homomorphic images of a given group G , one does not have to look at other groups and different homomorphisms. One can just concentrate on finding all normal subgroups H of G and studying G/H .

Impressive applications of other three ITs will appear throughout the course. They allow to reduce the study of groups of large orders to the ones of smaller orders, and to use induction.

Below we present several applications of The First IT.

1. Let $G = GL(n, \mathbb{F}_q)$, $H = \mathbb{F}_q^\times$ and $\phi(A) = \det A$. Then ϕ is a homomorphism, but the proof is not easy. It is equivalent to the theorem stating that $\det AB = \det A \det B$. For every $c \in H$, there exists $C \in G$ such that $\phi(C) = c$. Indeed, take $C = \text{diag}(c, 1, 1, \dots, 1)$. Hence ϕ is surjective. As $\ker \phi = SL(n, \mathbb{F}_q)$, we have $SL(n, \mathbb{F}_q) \trianglelefteq GL(n, \mathbb{F}_q)$, and

$$GL(n, \mathbb{F}_q)/SL(n, \mathbb{F}_q) \simeq \mathbb{F}_q^\times.$$

As a corollary we get

$$|SL(n, \mathbb{F}_q)| = |GL(n, \mathbb{F}_q)|/(q-1) = \frac{1}{q-1} \prod_{i=0}^{n-1} (q^n - q^i).$$

2. Let $G = S_n$, $H = \{-1, 1\}$ and $\phi(\pi) = 1$ if π is an even permutation, and $\phi(\pi) = -1$, if π is an odd permutation. The map ϕ is well-defined, since we have demonstrated that every element of S_n is either even or odd permutation. As you remember the proof of this fact was not trivial.

Then it is obvious that ϕ is a homomorphism, $\ker \phi = A_n$, and $A_n \trianglelefteq S_n$. As there are odd permutations for $n \geq 2$, e.g., transpositions, then ϕ is surjective. Hence $S_n/A_n \simeq \{-1, 1\}$, and the index of A_n in S_n , for $n \geq 2$, is 2.

In general, if $H \leq G$ and $|G : H| = 2$, then $H \triangleleft G$. Indeed, there exists $x \in G \setminus H$, and for every such x , $G = H \cup Hx$ and $G = H \cup xH$ are partitions of G . Hence $xH = Hx$. Since $hH = Hh$ for all $h \in H$, we have shown that for every $g \in G$, $gH = Hg$. Hence, $H \triangleleft G$.

3. Let $G = H = \mathbb{F}_q^\times$, and $\phi : G \rightarrow G$ is defined via $x \mapsto x^2$. Then ϕ is a surjective group homomorphism (obvious). The kernel of ϕ is the set of those $x \in G$, such that $x^2 = 1$. Since \mathbb{F}_q is a field, $x = 1$ or $x = -1$. Hence the subgroup of squares in G has index 2 for q odd, and there are $(q-1)/2$ of them. For q even, we get that every element of G is a square, and ϕ is an isomorphism in this case.

The statement also easily follows from the (deep) fact that G is cyclic.

Questions

Some of these questions may be hard, but they seem natural at this time.

- (i) Is it true that if $H \leq G$ and $|G : H| = 3$, then $H \triangleleft G$?
- (ii) Let $H \leq G$. Can both H and $(G : H)$ be infinite? For a given positive integer n , can we always find a group G and its nontrivial subgroup H such that $|G : H| = n$?
- (iii) Does the pair of groups H and G/H define G up to the isomorphism? More precisely, let A and B be two groups. We can always construct a group G having a normal subgroup N such that $A \simeq N$ and $B \simeq G/N$. How? Is such G defined uniquely by A and B ?

Assignment 4.

Read Sections 3.3 and 3.4 (including the discussion of simple groups, Hölder Program, and the Feit-Thompson Theorem).

Problems:

Sec. 3.3: 3, 4, 8.

Sec. 3.4: 1, 2.

Lecture 4 (a). Review.

Is there an analog of The Prime Factorization Theorem of integers for groups?

If the answer is 'Yes', then what is analog of a prime? of a product?

Let's begin with primes. It turns out that a reasonable analog is a **simple** group, which is defined as a non-trivial group with only two normal subgroups: $\langle e \rangle$ and G . An example is the cyclic group C_p , where p is prime, but there are others.

For a group-theoretic analog of the product of integers, one would, probably, try the direct product of groups. The example of C_9 , which is not isomorphic to $C_3 \times C_3$, shows that the analogy is not that clear.

Before proceeding to the theorem, we wish to make two remarks.

- Consider a dense sequence of embedded subspaces in an n -dimensional space:

$$V = V_n > V_{n-1} > \dots > V_1 > V_0 = \langle 0 \rangle, \quad \dim V_i = i.$$

The word dense here means that we cannot insert in this sequence any subspace W such that $V_{i+1} > W > V_i$ for some i .

Though there are many such sequences, their number of spaces is always $n + 1$, and all $V_{i+1}/V_i \simeq V_1$.

- Consider two sequence of factors of 60 ordered by divisibility with the quotients of successive terms being prime:

$$60 \succ 20 \succ 10 \succ 5 \succ 1, \quad \text{and}$$

$$60 \succ 30 \succ 15 \succ 3 \succ 1, \quad \text{and}$$

Then the multiset of the quotients of the first sequence is $\{\{3, 2, 2, 5\}\}$, and of the second $\{\{2, 2, 3, 5\}\}$. As we see they are equal.

Therefore is there an analog? Yes, but we leave it for the reader to judge how good it is. It is known as the Jordan-Hölder Theorem.

We will use the exposition by Martin Quick:

<http://www-groups.mcs.st-andrews.ac.uk/~martynt/teaching/5824/5824Groups4.pdf>

or by David Jao: <http://planetmath.org/>

There are versions for Jordan-Hölder Theorem for other algebraic structures, such as, e.g., some classes of modules and rings.

Lecture 5.

Consider the following statements and questions.

- (i) Let $Ax = b$ be a system of linear equations, where $A \in M_{m,n}(\mathbb{Z})$, $b \in \mathbb{Z}^m$. Determine whether it has solutions $x \in \mathbb{Z}^n$, and if it does find all of them.
- (ii) Let $GL_n(\mathbb{Z})$ denote the group of all $n \times n$ matrices over \mathbb{Z} with determinant 1 or -1 (**unimodular** matrices).

Let $A \in M_{m,n}(\mathbb{Z})$. There exist $L \in GL_m(\mathbb{Z})$ and $R \in GL_n(\mathbb{Z})$ such that

$$LAR = D = \text{diag}(d_1, d_2, \dots, d_s, 0, \dots, 0),$$

where $d_i > 0$, $i = 1, \dots, s$, and $d_i | d_{i+1}$, $i = 1, \dots, s-1$, and such a diagonal matrix is unique.

The theorem was proven by H.J.S. Smith in 1868, and the diagonal matrix on the left is called the **Smith normal form** of A . It was motivated by the problem (i) above, and provided its complete solution.

Transformation of A to D can be performed by using **elementary row (column) operations** of A and intermediate matrices which appear along the way. These are the following:

- interchange of two rows (columns)
- multiplication of a row (column) by -1
- replacing a row (column) by its sum with an integer multiple of another row (column).

Matrices L and R are products of matrices which correspond to the elementary transformations of rows and columns of A (in the order they are used in transforming A to D).

A numerical example illustrating the transformation of A to D , and its application to solving $Ax = b$ was distributed in class.

- (iii) Prove that any square matrix over \mathbb{C} is similar to a matrix having a Jordan canonical form, and such form is unique up to the interchange of the blocks.
- (iv) Prove that any square matrix over a field \mathbb{F} is similar to a matrix having a Rational canonical form, and such form is unique up to the interchange of the blocks.
- (v) Let $GL_n(\mathbb{R})$ be the general linear group over \mathbb{R} . It is defined as the group of bijective linear operators of the vector space $V = \mathbb{R}^n$, the operation is composition of operators. $GL_n(\mathbb{R})$ is isomorphic to the group of non-singular $n \times n$ matrices over \mathbb{R} (with respect to matrix multiplication). There are many isomorphisms between these groups, but each simply corresponds to a choice of a basis in \mathbb{R}^n .

Consider $M = \mathbb{Z}^n$ as \mathbb{Z} -module, where for any $m = (m_1, \dots, m_n) \in M$, and any $r \in \mathbb{Z}$, we define $rm = (rm_1, \dots, rm_n)$. For an associative ring R with 1, the definition of an R -module is the same as the definition of a vector space over a field, only “scalars” are taken from R . \mathbb{Z}^n can be thought as a discrete analog of \mathbb{R}^n . It forms what is called a lattice in \mathbb{R}^n , though the term “lattice” must be defined more formally. Examples of lattices appeared in number theory, in the studies of “algebraic integers”.

Examples are $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Z}\}$, or the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$.

An **isomorphism (or automorphism) of an R -module M** is a bijection $f : M \rightarrow M$ such that $f(x+y) = f(x)+f(y)$, and $f(rm) = rf(m)$ for all $x, y, m \in M$ and all $r \in R$. All automorphisms of M form a group under the composition.

Describe the group $\text{Aut}(\mathbb{Z}^n)$, where \mathbb{Z}^n is considered as \mathbb{Z} -module.

- (vi) Every finitely generated abelian group can be written as the direct sum of its cyclic subgroups. Under certain assumptions about these cyclic subgroups, the representation is unique. (This clearly covers the case of finite abelian groups).
- (vii) Every finitely generated module over a p.i.d. can be written as the direct sum of its cyclic submodules. Under certain assumptions about these cyclic submodules, the representation is unique.

We will see that statements/questions (i) – (vi) follow (or closely) related to (vii).

Suggested Exercises.

Problems vary in difficulty. Some are hard.

1. Find all solutions of $2x + 3y - 10z + 7u = -13$, where $(x, y, z, u) \in \mathbb{Z}^4$.

Hint: Review the theory of the linear diophantine equation $ax + by = c$, where a, b, c are fixed integers and $(x, y) \in \mathbb{Z}^2$. See, e.g., Theorem 9 in <http://www.math.udel.edu/~lazebnik/papers/ElementsThNum.pdf>.

2. Find all integer solutions of the system

$$2x + y + 4z = 17, \quad 5x - 2y - 6z = 13.$$

3. We know that in any vector space a product of a nonzero scalar and a nonzero vector is always a nonzero vector.

Give an example of a ring R and an R -module M such that there exist a nonzero $r \in R$ and nonzero $m \in M$ such that $rm = 0$.

Find several other statements from linear algebra which are correct in any vector space, but their analogs for modules may fail (in some modules).

4. Prove that neither the additive group of \mathbb{Q} , nor the multiplicative group of \mathbb{Q} is finitely generated. Are these two groups isomorphic?
5. Prove that for relatively prime m and n , we have the following isomorphism of additive groups:

$$\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$$

Can the statement hold for *some* m and n which are not relatively prime?

6. Are any of the following additive groups isomorphic:

$$\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}, \quad \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z}, \quad \text{and} \quad \mathbb{Z}/p^3\mathbb{Z},$$

where $p \geq 2$ is a positive prime integer? Consider the same question for $p \geq 4$ and not prime?

7. Is the additive group \mathbb{Z} a direct sum of two of its nontrivial proper subgroups? Consider the same question for the additive group of $\mathbb{Z}/p^n\mathbb{Z}$, p is a prime, n is a positive integer, and for the additive group of \mathbb{Q} .

8. Find (describe) the automorphism groups of the following *additive groups*:

$$\mathbb{Z}, \quad \mathbb{Z} \oplus \mathbb{Z}, \quad \mathbb{Q}, \quad \mathbb{Q} \oplus \mathbb{Q}, \quad \mathbb{Q}[\sqrt{2}], \quad \mathbb{Z}/n\mathbb{Z}$$

If your answer uses direct sums of familiar groups, describe these groups. Can these direct summands be represented as direct sums of their subgroups?

9. Find $\text{Aut}(D_{2n})$, where D_{2n} is the dihedral group (of order $2n$).

10. It is known that there are infinitely many automorphisms of the field of complex numbers \mathbb{C} . Can you name at least one nontrivial field automorphism of \mathbb{C} ?

Find (describe) the automorphism groups of the following *fields*:

$$\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{R}, \mathbb{R}(x).$$

11. (i) Find generators of a subgroup H in \mathbb{Z}^3 consisting of all (x_1, x_2, x_3) satisfying the conditions $x_1 + 2x_2 + 3x_3 = 0$, $x_1 + 4x_2 + 9x_3 = 0$.
(ii) Describe the structure of \mathbb{Z}^3/H .

Lecture 6.

- (i) The meaning of na , where $n \in \mathbb{Z}$ and $a \in A$ – an abelian group. This being understood, we have that any abelian group is a “natural” \mathbb{Z} -module.
- (ii) Let A be an abelian group. For $S \subset A$, by $\langle S \rangle$ we denote the smallest subgroup of A containing S as a subset. Of course, this is an “external” definition of $\langle S \rangle$. It is also clear that $\langle S \rangle$ is the intersection of all subgroups of A having S as a subset. The “internal” definition of $\langle S \rangle$ is this:

$$\langle S \rangle = \{k_1 s_1 + \cdots + k_n s_n : k_i \in \mathbb{Z}, s_i \in S, n \in \mathbb{N}\}.$$

If S is infinite, then only finite integral linear combinations of elements of S are considered.

If $\langle S \rangle = A$, we say that S **generates** A , and that S is a **generating set** of A . If A has a finite generating set, we say that A is **finitely generated**.

Examples.

- $\mathbb{Z} = \langle \{1\} \rangle = \langle \{5, 18\} \rangle$ (Why?);
 $\mathbb{Z} \neq \langle \{4, 10\} \rangle$. (Why?)
- $\mathbb{Z} \oplus \mathbb{Z} = \langle \{(1, 0), (0, 1)\} \rangle = \langle \{(2, 3), (5, 7)\} \rangle$ (Why?)
- The group $\mathbb{Z} \oplus \mathbb{Z}$ cannot be generated by one element. (Why?)
- $\mathbb{Z} \oplus \mathbb{Z} \neq \langle \{(3, 5), (-1, 2)\} \rangle$. (Why?)
- Neither $\mathbb{Z}[x]$, nor $C[0, 1]$ (the abelian group of the ring of all real continuous functions on $[0, 1] \subset \mathbb{R}$ is finitely generated abelian group. (Prove it.)

- (iii) We say that a nonempty subset $\{a_1, \dots, a_n\}$ of A is **linearly independent** if $k_1 a_1 + \cdots + k_n a_n = 0$ implies $k_1 = \cdots = k_n = 0$ (k_i are integers).

A finite linearly independent generating set in A , if it exists, is called a **basis** of A .

Examples.

- The residue class $[5]_8 \in A = \mathbb{Z}/8\mathbb{Z}$ generates A (why?). At the same time $\{[5]_8\}$ is not a linearly independent set in A : $8[5]_8 = [0]$ and integer 8 is not zero.
- $\{2\}$ is linearly independent in $A = \mathbb{Z}$, but $\langle \{2\} \rangle \neq \mathbb{Z}$.
- $\{-1\}$ is a basis of \mathbb{Z} , and $\langle \{(2, 3), (5, 7)\} \rangle$ is a basis of $\mathbb{Z} \oplus \mathbb{Z}$. (Why?)

- (iv) A finitely generated abelian group is **free** if it has a basis.

The following statements exhibit analogy between free abelian groups and vector spaces.

Theorem 11. *All bases of a finitely generated free abelian group A contain the same number of elements.*

A proof from Vinberg’s book was presented with all details filled. It was stressed that it uses some fundamental results about vector spaces (over \mathbb{Q}). Another key point of the proof is a “technical” results concerning linear dependence.

This allow to introduce the notion of the **rank** of a finitely generated free abelian group A , as the number of elements in any of its basis. It is denoted $\text{rk } A$. An important corollary of this theorem is that

Any finitely generated free abelian group A of rank n is isomorphic to \mathbb{Z}^n .

If $\{e_1, \dots, e_n\}$ is a basis of A , the mapping $f : A \rightarrow \mathbb{Z}^n$ defined by $e_i \mapsto (0, \dots, 0, 1, 0, \dots, 0)$ (1 is in the i th position), $i = 1, \dots, n$, is, clearly, an isomorphism. (Why?) This property is very similar to the fact that every n -dimensional vector space over a field \mathbb{F} is isomorphic (as a vector space) to \mathbb{F}^n .

Theorem 12. *Let $\{e_1, \dots, e_n\}$ be a basis of a free abelian group L , and*

$$(e'_1, \dots, e'_n) = (e_1, \dots, e_n)C$$

for some square integral matrix C of order n . Then elements e'_1, \dots, e'_n form a basis of L if and only if $\det C = \pm 1$.

A proof from Vinberg's book was presented with all details filled. It was stressed that it uses some fundamental results about determinants, and a well known (and not obvious at all) description of the entries of C^{-1} .

Lectures 7,8.

- (i) Here is another statement about free abelian groups which is similar to one about vector spaces.

Theorem 13. *Every subgroup N of a free abelian group of rank n is a free abelian group of rank at most n .*

The zero group is regarded as a free abelian group of rank 0. The proof from Vinberg's book is on induction on n . It is a rather natural argument, and it makes use of the fact that any subgroup of \mathbb{Z} is of the form $k\mathbb{Z}$ for some integer k . It seems like this special property of \mathbb{Z} has not been used before.

In an n -dimensional vector space, a proper subspace has dimension *strictly* less than n , and so it is not isomorphic (as vector space) to the ambient space. This is not true for free abelian groups: $2\mathbb{Z} < \mathbb{Z}$, but both have rank 1. As abelian groups they are isomorphic.

Everyone would agree that some basis of free abelian groups are nicer than others. For example, $\{(1, 4), (1, 2)\}$ and $\{(1, 0), (0, 2)\}$ are bases of the same subgroup H of \mathbb{Z}^2 (check!). The second basis immediately allows to write $H = \mathbb{Z} \oplus 2\mathbb{Z}$, a rather good description! It also implies that $\mathbb{Z}^2/H \cong \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ (or \mathbb{Z}_2 using a simplified notation) (check!). It is much harder to see both these facts when H is defined by its basis $\{(1, 4), (1, 2)\}$. Hence, a choice of a basis matters. It is also true that system of linear diophantine equations are trivial when the matrix of the system is diagonal. So, we have two natural questions:

- Is any system of linear diophantine equations $Ax = b$ equivalent to a system of linear diophantine equations $Dy = c$, where D is a diagonal matrix?
- Given a subgroup N of a finitely generated free abelian group A of rank n , is it always possible to choose a basis of A such that integer multiples of the vectors from this basis form a basis of N ?

We will see that these questions are very much related, and the following theorem will lead to answering both of them.

Theorem 14. *Every nonzero integral rectangular matrix $C = (c_{ij})$ can be reduced by integral row and column transformations to the diagonal form $D = \text{diag}(d_1, \dots, d_s, 0, \dots, 0)$, where all integers $d_i > 0$ and $d_i | d_{i+1}$ for all $i = 1, \dots, s-1$.*

Note that the diagonal form stated in the theorem is rather special. Why is this extra trouble? Let us comment on it later.

Our proof follows the one in Vinberg's book. Note that the statement of the theorem is slightly different than in his book (why did I change it?) The key idea is that the transformation allow to perform a sequence of divisions with remainder. At this point we use the property that in

addition of being an additive group, \mathbb{Z} is a *Euclidean ring*, where division with remainder and the Euclidean algorithm can be performed.

Each integral elementary transformations of rows or columns of a matrix can be achieved by a multiplication of this matrix by a very simple square matrix with determinant 1 or -1 . Multiplying these matrices, we obtain two square matrices L and R such that $LCR = D$.

Let $GL_n(\mathbb{Z})$ denote the group of all $n \times n$ unimodular matrices over \mathbb{Z} .

Theorem 15. *Let $A \in M_{m,n}(\mathbb{Z})$. There exist $L \in GL_m(\mathbb{Z})$ and $R \in GL_n(\mathbb{Z})$ such that*

$$LAR = D = \text{diag}(d_1, d_2, \dots, d_s, 0, \dots, 0),$$

where $d_i > 0$, $i = 1, \dots, s$, and $d_i | d_{i+1}$, $i = 1, \dots, s - 1$.

The result above allows easily to find a “diagonal” basis for a subgroup of a free abelian group.

Theorem 16. *Let A be a free abelian group of rank n , and let $N \leq A$. Then there exists a basis $\{e_1, \dots, e_n\}$ of A and positive integers d_1, \dots, d_s , $s \leq n$, such that $\{d_1e_1, \dots, d_se_s\}$ is a basis of N and $d_i | d_{i+1}$ for all $i = 1, \dots, s - 1$.*

The idea of the proof is to reduce this theorem to Theorem 15. We know that N is free of rank m (why?). Let $\{u_1, \dots, u_m\}$ be a basis of N , and $\{v_1, \dots, v_n\}$ be a basis of A . Then

$$(u_1, \dots, u_m) = (v_1, \dots, v_n)C$$

for some $n \times m$ integral matrix C . We transform each of the basis to another one (of the same group) by applying so called **integer elementary operations** on the vectors from the ordered bases. These are:

- interchange of two elements in an ordered basis
- multiplication of a basis element by -1
- replacing a vector from the basis by its sum with an integer multiple of another vector from the basis.

It is easy to check (do it!) that each of these operations replaces a basis of the group with another basis, as it does not affect linear independence of elements and their span. Perform an operation, and write the relation between the ordered bases again in the form

$$(\text{new ordered basis of } N) = (\text{old ordered basis of } A)C'$$

or

$$(\text{old ordered basis of } N) = (\text{new ordered basis of } A)C''.$$

The matrix C' differs from the matrix relating two old bases by an integer elementary transformation of its columns, and the matrix C'' – of its rows, and any integer elementary transformation of rows and columns can be obtained by a suitable change the bases. This means that a sequence of the integer elementary operations on bases of N and A can be chosen in a way which transforms matrix C into the diagonal form of Theorem 15.

As soon as such a form is obtained, the corresponding bases of A and N have the properties required in Theorem 16.

We are ready to prove the existence part of the main theorem on the structure of finitely generated abelian groups. It can be stated in several ways.

Theorem 17. (Invariant factors decomposition of a f.g.a.g.. Existence.) *Every nonzero finitely generated abelian group A is a direct sum of its finite cyclic and infinite cyclic subgroups:*

$$A \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_r,$$

such that all integers d_i are positive and $d_i | d_{i+1}$ for all $i = 1, \dots, s-1$.

If $d_1 = \cdots = d_q = 0$, then the first q summands have form $\mathbb{Z}/1\mathbb{Z} = \langle 0 \rangle$ and can be dropped.

The main ideas of the proof (from Vinberg's book): take a generating set $\{a_1, \dots, a_n\}$ of A , and define epimorphism (surjective homomorphism)

$$\phi : \mathbb{Z}^n \rightarrow A$$

via

$$(k_1, \dots, k_n) \mapsto k_1 a_1 + \cdots + k_n a_n.$$

For $N = \text{Ker } \phi$, find a basis e_1, \dots, e_n of \mathbb{Z}^n as in Theorem 16, and then show that

$$\psi : \mathbb{Z}^n \rightarrow \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_r$$

defined via

$$l_1 e_1 + \cdots + l_n e_n \mapsto ([l_1]_{d_1}, \dots, [l_s]_{d_s}, l_{s+1}, \dots, l_n),$$

is an epimorphism with $\text{Ker } \psi = N$. Hence $A \cong \mathbb{Z}^n / \text{Ker } \psi$ and is as stated in the theorem.

A **primary group** or a **p -group** is a finite group whose order is a power of a prime number p . Hence the order of every element of it is a power of p . (Why?)

We know that any finite cyclic group of order n , with the prime factorization of n being $n = p_1^{e_1} \cdots p_k^{e_k}$, is the direct sum of its primary cyclic subgroups $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$, or just $\mathbb{Z}_{p_i^{e_i}}$ for $i = 1, \dots, k$:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{e_k}}.$$

(Why?)

This leads to the following theorem.

Theorem 18. (Primary decomposition of a f.g.a.g.. Existence.) *Every finitely generated abelian group A is a direct sum of its primary cyclic and infinite cyclic subgroups.*

Lecture 9.

- (i) The proofs of uniqueness of decompositions in algebra are often not trivial. For example, if the existence of the prime factorization of integers follow only from their multiplicative properties and the Well-Ordering axiom, the proof of uniqueness must use more. See, e.g., D. Hilbert's argument in Section 6 of
<http://www.math.udel.edu/~lazebnik/papers/ElementsThNum.pdf>
- (ii) The proof of the Uniqueness of the Primary decomposition of a f.g.a.g. (Theorem 18) from Vinberg's book was distributed in class at the end of Lecture 3.
- (iii) The condition $d_i|d_{i+1}$ was not used in the proof of Theorem 18. But it can be used now to prove the uniqueness of the sequence of d_i in Theorem 17. We show that the numbers d_1, \dots, d_s of Theorem 17 can be reconstructed from the orders of finite primary cyclic subgroups in Theorem 18 *uniquely* (in the handout from Vinberg's book, page 336). It is a brief version of the following argument.

The primary decomposition of the torsion subgroup of A , $\text{Tor } A$, was obtained by first representing it as the direct sum of \mathbb{Z}_{d_i} , then taking the prime factorization of $d_i = p_{i1}^{k_{i1}} \cdots p_{iq(i)}^{k_{iq(i)}}$, and then representing \mathbb{Z}_{d_i} as the direct sum $\mathbb{Z}_{p_{ij}}^{k_{ij}}$, $j = 1, \dots, q(i)$. Therefore every cyclic primary subgroup of $\text{Tor } A$ appears as a direct summand of some of \mathbb{Z}_{d_i} , and its order divides some d_i . Let p^{e_p} be the largest order of a cyclic p -group which appears in the primary decomposition of $\text{Tor } A$. Since it divides at least one of d_i , and $2 \leq d_1|d_2 \cdots |d_s$, it must divide d_s . This holds for every prime dividing the order of $\text{Tor } A$. Hence d_s is the product of such powers, and so it is determined uniquely (based on the fact that we know that the decomposition of $\text{Tor } A$ into primary cyclic group is unique).

Note that the the order of $\text{Tor } A$ can be divisible by a larger power of p than p^{e_p} . For example, if

$$\text{Tor } A = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \cdots ,$$

then we claim that d_s is divisible by 2^2 , though $|\text{Tor } A|$ is divisible by 2^4 .

Now it is clear that d_{s-1} must be divisible by the next largest power of p (it may be equal to p^{e_p}), for every power of p which appears as the order of a direct summand of the primary cyclic decomposition of $\text{Tor } A$. And so on. This gives the reconstruction.

Corollary 2. *All d_i of Theorem 17 are uniquely defined.*

This explains the adjective **invariant** in the **invariant factors**, the term used for d_1, \dots, d_s .

Corollary 3. $|\text{Tor } A| = d_1 \cdots d_s$. *The last invariant factor d_s is divisible by every prime dividing $|\text{Tor } A|$.*

Corollary 4. *Every finite abelian group has a unique decomposition into the direct sum of its finite cyclic subgroups corresponding to its invariant factor, as well as the unique decomposition into the direct sum of its primary cyclic subgroups.*

- (iv) The **exponent** of any group G is the smallest positive integer n such that $g^n = e$ for every $g \in G$, if such n exists. If there is no such n , we say that the exponent of G is ∞ . If G is abelian and the additive notations are used, $g^n = e$ corresponds to $ng = 0$.

If G is a finite abelian group, then it is easy to show that its exponent is the least common multiple of the orders of all its elements. (Can you do it? Let a and b be two elements of an abelian group G , of orders m and n , respectively. Prove that the order of ab is the least common multiple of m and n , i.e., the smallest positive integer which is divisible by both m and n .)

Corollary 5. *The exponent of a finite abelian group is equal to its greatest invariant factor d_s .*

Proof: Let G be such a group. Consider the invariant factors decomposition of G : $G = \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_s}$, $2 \leq d_1 | d_2 | \cdots | d_s$. Then every element of G can be thought as $g = (g_1, \dots, g_s)$, where $g_i \in \mathbb{Z}_{d_i}$ for all i . Then $|g_i|$ divides d_i which divides d_s , and so $d_s g_i = 0$ for all i . This makes $d_s g = 0$. Hence, $|g|$ divides d_s , and the exponent of G is at most d_s . But G contains an element of order d_s , namely the generator of \mathbb{Z}_{d_s} , e.g., $[1]_{d_s}$ (or $([0]_{d_1}, \dots, [0]_{d_{s-1}}, [1]_{d_s})$), if we wish to continue thinking about G as the direct sum. Therefore, the exponent of G is at least d_s . Hence it is d_s . \square

Corollary 6. *The exponent of a finite abelian group is equal to its order if and only if the group is cyclic.*

Proof: A finite abelian group G is cyclic if and only if there exists only one summand in its invariant factor decomposition (we are using the uniqueness of such a decomposition). This happens if and only if $G = \mathbb{Z}_{d_s}$, which is equivalent that the exponent of G is equal to its order. Both are equal d_s . \square

- (v) The following fact is fundamental, especially when it is used for finite fields.

Theorem 19. *Every finite subgroup of a multiplicative group of a field is cyclic. In particular, the multiplicative group of a finite field is cyclic.*

Proof: Let G be a finite subgroup of the multiplicative group \mathbb{F}^* of a field \mathbb{F} , and let m be the exponent of G . Then $g^m = 1$ for all $g \in G$. But the polynomial $x^m - 1$ has at most m roots in \mathbb{F} . Hence, $|G| \leq m$. On the other hand, as $g^{|G|} = 1$, from the definition of the exponent of a group we get $m \leq |G|$. Hence $m = |G|$, and G is cyclic by Corollary 6 \square

Lecture 10.

- (i) A complete analogy of the definition of a (left/right) module and a vector space. We get a vector space if the ring is a field (by definition).

Definition of a submodule. Important examples:

- Every abelian group is a \mathbb{Z} -module.
- Every left ideal in a ring A is an A -module. In particular, A itself is both left and right module over A .
- Every vector space is a module over the ring $L(V)$ of all linear operators on V .
- Given a vector space V over a field \mathbb{F} . Fix a linear operator $T : V \rightarrow V$. For every polynomial $f(t) = a_0 + a_1t + \cdots + a_nt^n \in \mathbb{F}[t]$, consider the corresponding linear operator $f(T) = a_0id + a_1T + \cdots + a_nT^n \in L(V)$. Define an action of $\mathbb{F}[t]$ on V by

$$fv = f(T)(v), \quad f \in \mathbb{F}[t], \quad v \in V.$$

It is clear that this defines V as an $\mathbb{F}[t]$ -module.

It is clear that this definition depends heavily on a choice of T .

- We can say that in the previous example, as soon as we know how the indeterminate t acts on V , the action of the whole ring $\mathbb{F}[t]$ is completely defined. Any subspace of V invariant with respect to the action of t is a submodule. So if T “represents” t , then any $\mathbb{F}[t]$ -submodule of V is an invariant subspace of T .
- (ii) An important moment in the definition of a factor module M/N : the action of the ring on the cosets $x + N$ is defined as

$$a(x + N) = ax + N,$$

rather than $a(x + N) = ax + aN$.

- (iii) Definition of a module homomorphism $f : M \rightarrow M'$, and a module isomorphism. (Similar to linear maps of vector spaces). The **canonical** homomorphism $M \rightarrow M/N$, where N is a submodule of M :

$$\pi : M \rightarrow M/N, \quad x \mapsto x + N.$$

π is an epimorphism, and $\text{Ker } \pi = N$.

- (iv)

Theorem 20. (Module Homomorphism Theorem) *Let $f : M \rightarrow N$ be a homomorphism of A -modules. Then*

$$\text{Im } f \cong M/\text{Ker } f,$$

and the isomorphism can be defined as

$$\phi : y = f(x) \mapsto \phi(x) = x + \text{Ker } f.$$

Note that for a $y \in f(M)$, there may be several different x such that $f(x) = y$. Therefore, strictly speaking, one has to check that ϕ is well defined (which is very easy). Please, write a proof of this theorem.

- (v) Definitions of: a linear combination of finitely many elements of a module; submodule generated by a subset S of a module; a generating set of a module; a finitely generated module. All these definitions are similar to the ones in abelian groups or in vector spaces.

A **cyclic** A -module is an analogy of a cyclic subgroup of an abelian group, or a span of a vector in a vector space, or a principal ideal in A : for $m \in M$, the cyclic module generated by m is $Am = \{am : a \in A\}$.

- (vi) The following ideal of A plays an important role in module theory:

$$\text{Ann } M = \{a \in A : aM = 0\},$$

where aM is understood as the set $\{am : m \in M\}$. It is easy to check that $\text{Ann } M$ is indeed a left ideal in A . It is called the **annihilator** of M .

It is important to note that though M may be a left A -module, $\text{Ann } M$ is always a 2-sided ideal in A . Indeed, let $a \in \text{Ann } M$ and $b \in A$. Then, for any $m \in M$, $(ab)m = a(bm) = am'$ for some $m' \in M$, as M is a left A -module. As $a \in \text{Ann } M$, $am' = 0$, and therefore $(ab)M = 0$. This implies that $ab \in \text{Ann } M$. The fact that $ba \in \text{Ann } M$ is trivial. Hence, $b(\text{Ann } M) \subset \text{Ann } M$, and $(\text{Ann } M)b \subset \text{Ann } M$ for all $b \in A$. This means that $\text{Ann } M$ is a 2-sided ideal of A .

How can one understand ALL cyclic modules over A ? The following theorem explains that in order to do it, one does not have to “leave” A , and think about all possible m ’s in all possible M ’s. The answer is “within” A .

Theorem 21. (Cyclic Module Theorem) *Every cyclic A -module M is isomorphic to a module A/I , where I is a left ideal of the ring A . If A is commutative, $I = \text{Ann } M$, and thus it is defined by M uniquely.*

The idea of a simple proof is: if $M = \langle x \rangle$ is a cyclic A -module, then the map

$$f : A \rightarrow M, \quad a \mapsto ax$$

is a module epimorphism. Now use Theorem 20. Finish the proof. How the commutativity of A is used? Did we have a similar result for abelian groups?

- (vii) Definition of: linear independence of a finite set of elements of an A -module M (over A); of a (finite) basis of a module; of a free module as module with a basis. All this is similar to the corresponding definitions in abelian groups. It follows that a free cyclic module is isomorphic to A (same for abelian groups).
- (viii) In order to continue with the theory of finitely generated modules, we need special rings. How special? For example, PID’s will work. They are fields (which are PID’s), \mathbb{Z} and $\mathbb{F}[t]$ (\mathbb{F} is a field) (which are even Euclidean rings). PID’s have an additional nice properties that prime and irreducible elements are the same, there gcd of two elements exist and can be represented as a linear combination of the element. Also there exists unique prime factorization in them.

It is not easy to give example of a ring which is PID but not Euclidean. One of such is $\{a + b\frac{1+\sqrt{-19}}{2} : a, b \in \mathbb{Z}\}$, but a proof is not easy (it can be found in Dummit and Foote's text).²

All applications we are concerned with are over \mathbb{Z} , and $\mathbb{F}[x]$, where \mathbb{F} is a field. The cases of modules over \mathbb{F} are special cases, to which other cases reduce. That is why usually linear algebra is studied first. If we can assume that our ring A is one of them, the modification of proofs compared with the abelian groups will be minimal.

(ix)

Theorem 22. *All bases of a free A -module M contain the same number of elements.*

Why cannot we prove this theorem like the analogous statement for abelian groups? What does not work?

The proof in Vinberg's text goes like this. If A is a field, we are done by quoting the corresponding result from linear algebra for vector spaces. If A is not a field, then there exists a prime element in A , call it p . It is easy to check that L/pL is a module over $A/pA = A/(p)$, and, since $A/(p)$ is a field, L/pL is a vector space over $A/(p)$. Let $\{e_1, \dots, e_n\}$ be a basis of L over A . One can show that $\{[e_1], \dots, [e_n]\}$ is a basis of L/pL over $A/(p)$. (Do it! It is a useful exercise.)

So rank of L is equal to the dimension of the vector space L/pL over $A/(p)$, which is clearly independent of the choice of a basis of L .

- (x) As before we obtain: the theorem that any submodule N of a free A -module M is free and of no greater rank; the theorem about the existence of a special basis of N which brings the relation matrix between bases of N and M to the Smith normal form (over Euclidean rings the argument is completely analogous to the one over \mathbb{Z}); and the Invariant Factors Canonical form for the structure of a finitely generated A -module:

$$M \cong A/(d_1) \oplus A/(d_2) \oplus \dots \oplus A/(d_s) \oplus A^r, \quad (0.1)$$

where d_i are not units (noninvertible) elements of A , and $d_i | d_{i+1}$ for $i = 1, \dots, s-1$.

- (xi) From the Invariant Factors Canonical form, we get the theorem of the direct sum decomposition into primary cyclic submodules. The collection of the annihilators for these primary free cyclic submodules is defined uniquely. The base for this transition is the fact that in PID there exists a unique prime decomposition, and for $(u, v) = 1$,

$$A/(u, v) \cong A/(u) \oplus A/(v). \quad (0.2)$$

For the uniqueness, see the corresponding pages from Vinberg. Instead of the order of the torsion group of an abelian group, he uses the dimension of $\{m \in M : px = 0\}$ as a vector space over $A/(p)$.

²Examples of PID's which are not Euclidean rings can be found in the rings of algebraic integers of the complex quadratic extensions $\mathbb{Q}[\sqrt{-D}]$, with positive integer D coming ONLY from the set $\{19, 43, 67, 163\}$ – a famous result. Part of it was known to Gauss, but the proof by Stark/Heegner was published in 1969.

- (xii) If $\text{Ann } M \neq 0$, M is called **periodic**. For a periodic module, $r = 0$ (A contains 1), and so $\text{Ann } M = (d_s)$ (why?). Assume M is periodic.

If $A = \mathbb{F}[t]$, d_i is a monic polynomial generating the ideal (d_i) . The A -module in this case is a vector space over \mathbb{F} , and since M is periodic, the vector space is finite dimensional. Call it V . Let T be a linear operator on V . Let indeterminate t act on V via T , and this defines the action of $\mathbb{F}[t]$ on V . But the action of t on V reduces to the action of t on the factor rings of the form $\mathbb{F}[t]/(f)$, where $f = f_0 + f_1t + \cdots + f_{k-1}t^{k-1} + t^k$. This action is easy to understand, and this is how we get the canonical forms for T !

Lecture 11.

The proofs of all statements of the theorems of this lecture follow from what we already studied almost immediately. For more details and very careful exposition, see the text by Dummit and Foote, Sections 12.12 and 12.13.

Let us repeat the main idea again: the action of a linear operator T on a vector space V is mimicked by the action of indeterminate t on the $\mathbb{F}[t]$ -module M . M is actually V . The reason we call it by a different letter is to stress the fact that we view it as an $\mathbb{F}[t]$ -module. Decomposition of V in a direct sum of invariant spaces corresponds to the decomposition of M into a direct sum of submodules. Now, for M we know about the existence of a very special decomposition, namely (0.1). By studying the action of t on a certain bases of the cyclic submodules of this decomposition, and translating the results to the action of T on the corresponding special bases of V , we get the so called the Canonical Rational Form for T .

- (i) **Rational Canonical Form of a matrix.** Note that $\mathbb{F}[t]/(f)$ is a vector space over \mathbb{F} , with a basis $\{[1], [t], \dots, [t^{k-1}]\}$, where $[t^i] = [t^i]_f = t^i + (f)$. The operator “multiplication by t ” acts on this basis as

$$\begin{aligned} 1 + (f) &\mapsto t + (f) \\ t + (f) &\mapsto t^2 + (f) \\ &\dots \quad \dots \quad \dots \\ t^{k-2} + (f) &\mapsto t^{k-1} + (f) \\ t^{k-1} + (f) &\mapsto t^k + (f) = -f_0 - f_1t - \cdots - f_{k-1}t^{k-1} + (f) \end{aligned}$$

This means that the matrix of the “multiplication by t ” operator in basis $\{[1], [t], \dots, [t^{k-1}]\}$ is

$$C(f) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 1 \\ -f_0 & -f_1 & -f_2 & \cdots & -f_{k-1} \end{pmatrix}$$

The $k \times k$ matrix $C(f)$ is called the **companion** matrix of f . Using the decomposition of M (0.1) into the direct sum of cyclic modules, we obtain the following theorem.

Theorem 23. (a) For every linear operator T of an n -dimensional vector space V , there exists a basis of V such that the matrix of T in this basis is block-diagonal, with blocks being the companion matrices of polynomials $d_i(t)$, $i = 1, \dots, s$, and $d_1|d_2|\dots|d_s$. Also, $n = \deg d_1 + \deg d_2 + \dots + \deg d_s$.

- (b) For every square $n \times n$ matrix A over \mathbb{F} , there exists an invertible matrix C over \mathbb{F} such that $C^{-1}AC$ the matrix described in the previous part, called the **Rational Canonical form** of A . Polynomials d_i are called the **invariant factors** of A , and are defined by A uniquely.
- (c) The monic polynomial d_s is the minimal polynomial of T (or of A).
- (d) The characteristic polynomial $|tI_k - C(f)|$ of $C(f)$ is f (check it!!!). This implies that the characteristic polynomial $|tI_n - A|$ of A is equal to the product of all invariant factors of A , i.e., $d_1 \cdot d_2 \cdot \dots \cdot d_s$.
- (e) (Generalization of Cayley-Hamilton theorem.) *Minimal polynomial of A divides its characteristic polynomial. (Hence, A is annihilated by its characteristic polynomial, which is the usual statement of the Cayley-Hamilton theorem.) Moreover, the minimal and the characteristic polynomial of A have exactly the same roots (but their multiplicity may differ). Hence, the characteristic polynomial divides the power of its minimal polynomial.*

Note that in order to transform A to its rational canonical form, we perform all transformations over the base field \mathbb{F} . That explains the term “rational”.

The minimal polynomial of T (or A) is analogous to the exponent of a finite abelian group, while the characteristic polynomial is an analog of the order of the group.

- (ii) **Jordan Canonical Form of a matrix.** Let \mathbb{F} be algebraically closed. Factoring each polynomial d_i in (0.1) into the product of linear factors over \mathbb{F} , and using (0.2), we obtain the decomposition of a periodic module M into the direct sum of cyclic $\mathbb{F}[t]$ -modules of the form $\mathbb{F}[t]/((t - \lambda)^k)$.

Note that $\mathbb{F}[t]/((t - \lambda)^k)$ is a vector space over \mathbb{F} , with a basis $\{[1], [t - \lambda], \dots, [(t - \lambda)^{k-1}]\}$, where $[(t - \lambda)^i] = [(t - \lambda)^i] = (t - \lambda)^i + ((t - \lambda)^k)$. The operator “multiplication by $t = \lambda + (t - \lambda)$ ” acts on this basis as

$$\begin{aligned} 1 + ((t - \lambda)^k) &\mapsto \lambda \cdot 1 + 1 \cdot (t - \lambda) + ((t - \lambda)^k) \\ (t - \lambda) + ((t - \lambda)^k) &\mapsto \lambda \cdot (t - \lambda) + 1 \cdot (t - \lambda)^2 + ((t - \lambda)^k) \\ &\dots \quad \dots \quad \dots \\ (t - \lambda)^{k-2} + ((t - \lambda)^k) &\mapsto \lambda \cdot (t - \lambda)^{k-2} + 1 \cdot (t - \lambda)^{k-1} + ((t - \lambda)^k) \\ (t - \lambda)^{k-1} + ((t - \lambda)^k) &\mapsto \lambda \cdot (t - \lambda)^{k-1} + ((t - \lambda)^k) \end{aligned}$$

This means that the matrix of the “multiplication by t ” operator in basis $\{[1], [t - \lambda], \dots, [(t - \lambda)^{k-1}]\}$ is

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}$$

The $k \times k$ matrix $J_k(\lambda)$ is called the **Jordan** matrix of f . Using the decomposition of M (0.1) into the direct sum of cyclic modules $\mathbb{F}[t]/((t - \lambda)^k)$, we obtain the following theorem.

Theorem 24. (a) *For every linear operator T of an n -dimensional vector space V , there exists a basis of V such that the matrix of T in this basis is block-diagonal, with blocks being the Jordan matrices of polynomials $(t - \lambda)^k$, which appear in the decompositions of polynomials d_i , $i = 1, \dots, s$, into powers of distinct linear factors. The sum of degrees of all these powers is n .*

(b) *For every square $n \times n$ matrix A over \mathbb{F} , there exists an invertible matrix C over the splitting field of \mathbb{F} such that $C^{-1}AC$ is the matrix described in the previous part, called the **Jordan Canonical form** of A . Polynomials $(t - \lambda)^k$ are called the **the elementary divisors** of A , and are defined by A uniquely.*

(c) *For a given λ , the factors of the form $(t - \lambda)^k$ may appear in factorizations of several polynomials d_i . Then the one of the largest power divides the minimal polynomial of T (or of A). Hence, the minimal polynomial is the product of such powers over all distinct λ .*

(d) *The characteristic polynomial $|tI_k - J_k(\lambda)|$ of $J_k(\lambda)$ is $(t - \lambda)^k$. This implies that the characteristic polynomial $|tI_n - A|$ of A is equal to the product of all elementary divisors of A .*

(e) (Generalization of Cayley-Hamilton theorem.) *Minimal polynomial of A divides its characteristic polynomial. (Hence, A is annihilated by its characteristic polynomial, which is the usual statement of the Cayley-Hamilton theorem.) Moreover, the minimal and the characteristic polynomial of A have exactly the same roots (but their multiplicity may differ). Hence, the characteristic polynomial divides the power of its minimal polynomial.*

Note that if \mathbb{F} is not algebraically closed, the Jordan Canonical form of a matrix over \mathbb{F} has entries from the splitting field of \mathbb{F} .

Again, the minimal polynomial of T (or A) is analogous to the exponent of a finite abelian group, while the characteristic polynomial is an analog of the order of the group.

The invariant factors of T (or A) can be computed from its elementary divisors in the same way as it was done for abelian groups.

(iii) **How does one compute the canonical forms of a matrix?**

One way is to first find the invariant factors. This leads to the Rational Canonical form. Then, if one can factor each invariant factor into the product of linear polynomials, one obtains all elementary divisors, and so can write the Jordan Canonical form.

How does one find the invariant factors of A ? In order to do it, one can perform the elementary row and column operations on the matrix $tI - A$, considered as a matrix over $\mathbb{F}[t]$, and bring it to the Smith Normal form with all diagonal entries are 1 or monic polynomials. Then all diagonal entries different from 1, will give the invariant factors of A !

Why?

As in the proofs of Theorem 17 and its analog for finitely generated modules over a PID, the invariant factors appear when a special basis of the $\text{Ker } \phi$ of the epimorphism $\phi : A^n \rightarrow M$ is found. We remind the reader that A^n is (free) A -module of rank n , A is a PID, M is an A -module over A generated by n elements.

Let T be a linear operator on a vector space V over \mathbb{F} of dimension n . Let $A = (a_{ij})$ represent T in some ordered basis (v_1, \dots, v_n) . So

$$T(v_i) = \sum_{j=1}^n a_{ij} v_j.$$

The action of $\mathbb{F}[t]$ on V is completely defined by the action of $t \in \mathbb{F}[t]$ on V via $tv = T(v)$. For basis vectors v_i , this gives $tv_i = \sum_{j=1}^n a_{ij} v_j$. Let $v'_i = -a_{i1}v_1 - \dots - a_{i,i-1}v_{i-1} + (t - a_{ii})v_i - a_{i,i+1}v_{i+1} - \dots - a_{in}v_n$.

Obviously, all v'_i are in the kernel, and it is easy to argue that they span it. As we have

$$(v'_1, \dots, v'_n) = (v_1, \dots, v_n)(tI - A),$$

$tI - A$ is the transition (or relation) matrix between these bases. Similarly to what we have done for the abelian groups, finding the invariant factors of V as a $\mathbb{F}[t]$ -module can be done by transforming matrix $tI - A$ to the Smith Canonical form by using the elementary row and column operations.

Suggested Exercises. Set 2.

Problems vary in difficulty. Some may be hard.

1. Prove that a group is finite if and only if it has finitely many subgroups.
2. Prove that the converse of the Lagrange's theorem holds for finite abelian groups: for positive integers m and n , if $|G| = n$ and $m|n$, then G has a subgroup of order m .
3. Find a generator of \mathbb{Z}_7^* , \mathbb{Z}_{41}^* , and $(\mathbb{Z}_2[x]/(x^3 + x + 1))^*$, where $(x^3 + x + 1)$ denotes the principal ideal in $\mathbb{Z}_2[x]$ generated by $x^3 + x + 1 \in \mathbb{Z}_2[x]$.
4. Describe all finite multiplicative subgroups of the multiplicative groups of the following fields:

$$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, \mathbb{F}_{13}, \mathbb{F}_{27}, \mathbb{Q}[\sqrt{2}].$$

What are their generators?

Hint: if a number $z \in \mathbb{C}^*$ has a finite order, what is $|z|$?

5. Let $U = \{z \in \mathbb{C} : |z| = 1\}$. Then U is a multiplicative group.
 - (i) Explain that U contains uncountably many elements of infinite order.
 - (ii) Show that $u = e^{i\alpha}$, where $\alpha = \arccos(1/3)$, has infinite order in U . (*Hint:* Study $\cos n\alpha$ and $\sin n\alpha$ for $n = 1, 2, 3, \dots$)
6. If the multiplicative group of a field is cyclic, should the field be necessarily finite?
7. What is the automorphism group of the additive group of all polynomials with integer coefficients of degree at most n ?
What if the coefficients come from \mathbb{Q} , or from \mathbb{R} ?
8. What can be said about the orders of elements of the group \mathbb{Q}/\mathbb{Z} ? (the factor group of the additive group of \mathbb{Q} by its subgroup \mathbb{Z}). Is this group finitely generated?
9. (i) Prove that $f : \mathbb{Q} \rightarrow \mathbb{C}^*$ given by $r \mapsto e^{2\pi ir}$ is a homomorphism. What is the image of f ? What is the kernel of f ?
(ii) Prove that \mathbb{Q}/\mathbb{Z} is isomorphic to the group of all roots of unity in \mathbb{C} .
(iii) Prove that for any nonzero $r \in \mathbb{Q}$, $\mathbb{Q}/\langle r \rangle \cong \mathbb{Q}/\mathbb{Z}$.
10. Is it true that if every proper subgroup of a group is finite, the group itself is finite?
Does the answer change if the group is abelian?
11. Any cyclic group (finite or infinite) has the property that every proper subgroup of it is cyclic. In this problem we consider an example of a non-cyclic infinite group with the property that every subgroup of the group is finite and cyclic.

Let p be a fixed prime integer. For every positive integer $n \geq 1$, let C_{p^n} denote the multiplicative group of all roots of unity of degree p^n , and let

$$C_{p^\infty} := \bigcup_{n=1}^{\infty} C_{p^n}.$$

- (a) Check that $C_p < C_{p^2} < C_{p^3} < \dots < C_{p^n}$.
- (b) Prove that C_{p^∞} is not cyclic, and that each of its proper subgroup is finite and cyclic.

Comment. The group C_{p^∞} (other notations for it are $\mathbb{Z}[p^\infty]$, $\mathbb{Z}/p^\infty\mathbb{Z}$, or \mathbb{Z}_p^∞) is often called **quasicyclic**, and it appears in classification of some classes of infinite abelian groups. It is known that every infinite abelian group which has all proper subgroup finite must be (isomorphic to) C_{p^∞} . Existence of infinite non-abelian groups which have every proper subgroup finite is open, as far as I know, and is known as O.Y. Schmidt problem.

12. Can G be infinite, but have the order of each of its elements is no more than a fixed number n ?
13. What is the automorphism group of the additive group of all polynomials with integer coefficients of degree at most n ?
What if the coefficients come from \mathbb{Q} , or from \mathbb{R} ?
14. If every element of a finite group G has order which is a power of a fixed prime p (orders of distinct elements can be distinct powers of p), should the order of the group G be a power of p ?
Does it matter whether G is abelian or not?
15. Find a basis for the submodule of \mathbb{Z}^3 generated by $f_1 = (1, 0, 1)$, $f_2 = (2, -3, 1)$, $f_3 = (0, 3, 1)$ and $f_4 = (3, 1, 5)$.
16. Find a basis for the submodule of $\mathbb{Q}[x]^3$ generated by $f_1 = (2x-1, x, x^2+3)$, $f_2 = (x, x, x^2)$, and $f_3 = (x+1, 2x, 2x^2-3)$.
17. Determine the structure if \mathbb{Z}^3/K , where K is generated by $f_1 = (2, 1, -3)$ and $f_2 = (1, -1, 2)$.
18. Let $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ be defined as $f((x, y)) = (28x + 38y, 12x + 16y)$. Find the index of $\text{Im}(f)$ in \mathbb{Z}^2 and describe $\mathbb{Z}^2/\text{Im}(f)$.
19. Let $f : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ be a \mathbb{Z} -linear map, and let $A \in M(n, \mathbb{Z})$ be a matrix of f in some basis. Suppose A has rank n (over \mathbb{Q} , and, hence, over \mathbb{Z}). Prove that the index of $f(\mathbb{Z}^n)$ in \mathbb{Z}^n is equal to $|\det(A)|$.
20. Prove that a system of linear equations with n variables has a solution in integers if and only if the corresponding system of congruences modulo n has a solution for all integers $n \geq 1$.

Comment. The result is not correct for nonlinear equations: e.g., for each $n \geq 1$, the congruence $(2x+1)(3x+1) \equiv 0 \pmod{n}$ has a solution (can you prove this?), while the equation $(2x+1)(3x+1) = 0$ has no solution in integers.

21. Let $S = \{s_1, \dots, s_m\}$ be a linearly independent set of vectors in \mathbb{R}^n . The additive subgroup $L = \langle S \rangle$ of \mathbb{R}^n generated by S is called the **lattice** generated by S . A **fundamental domain** $T = T(S)$ of the lattice L is defined as

$$T = \left\{ \sum_{1 \leq i \leq m} x_i s_i : 0 \leq x_i < 1, x_i \in \mathbb{R} \right\}.$$

The **volume** $v(T)$ of T is defined in the usual way, as the square root of the absolute value of the determinant of an $m \times m$ matrix whose i -th row is s_i . Though T itself depends on a particular set of generators of L , the volume of T does not! Prove the following statement.

Let $S = \{s_1, \dots, s_m\}$ and $U = \{u_1, \dots, u_t\}$ be two sets of linearly independent vectors which generate the same lattice L . Then $m = t$ and $v(T(S)) = v(T(U))$.

22. If M is an abelian group, M is a \mathbb{Z} -module, with the usual action of \mathbb{Z} on M . Can this action of \mathbb{Z} on M be extended to make M into a \mathbb{Q} -module?
23. Let M be the ideal in $\mathbb{Z}[x]$ generated by 2 and x . Show that M is not a direct sum of cyclic $\mathbb{Z}[x]$ -modules.

(This generalizes the fact that the ideal $(2, x)$ in $\mathbb{Z}[x]$ is not principal.)

24. Let D be the Smith normal form of an integer square matrix A . Prove or give counterexamples to the following statements.
- (i) D and A have equal traces.
 - (ii) D and A have equal determinants.
 - (iii) D and A similar matrices, i.e., $C^{-1}AC = D$ for some square matrix C .

25. Write all possible sequences of invariant factors for 3 matrices over \mathbb{Z}_2 and the corresponding rational forms.

(For a matrix $A \in M(3, \mathbb{Z}_2)$, the invariant factors come from $xI - A$.)

26. How many conjugate classes does the group $GL(3, \mathbb{Z}_p)$ have, where p is a prime?

Lecture 12.

Elements of a group (or a ring, or a field) can ‘act’ on elements of a non-empty set. For example, \mathbb{F}^\times acts on vectors from any vector space V over \mathbb{F} , e.g., on \mathbb{F}^n , via multiplication by scalars, when $k \in \mathbb{F}^\times$ maps a vector v to another vector kv . The symmetric group S_n can be thought acting on the set $[n]$. Group $GL(n, \mathbb{F})$ acts on V : $f \in GL(n, \mathbb{F})$ maps every $v \in V$ to $f(v)$.

These, and many other examples of a group acting on a set, are captured in the following definition.

Let G be a group, and let X be a non-empty set. We refer to elements of X as **points**. Let $f : G \times X \rightarrow X$ be such that

- $f((g_2g_1, x)) = f((g_2, f((g_1, x))))$ for all $g_1, g_2 \in G$ and all $x \in X$;
- $f((e, x)) = x$ for all $x \in X$.

Then f is called an **action** of G on X . To avoid many parenthesis, let us denote $f((g, x))$ by $g \cdot x$ or x^g . Then the two requirements on f can be rewritten as:

- $(g_2g_1) \cdot x = g_2 \cdot (g_1 \cdot x)$ for all $g_1, g_2 \in G$ and all $x \in X$;
- $e \cdot x = x$ for all $x \in X$.

If we use exponential notations, we get $x^{g_1g_2} = (x^{g_1})^{g_2}$ and $x^e = x$.

Let G act on X . Fix $g \in G$, and consider a map $\sigma_g : X \rightarrow X$ defined by $x \mapsto x^g$.

Proposition 2. σ_g is a bijection on X , i.e., $\sigma_g \in \text{Sym}(X)$.

Proof. Left for the reader □

Let G act on X , and for $g \in G$, let σ_g be defined as above. Consider a map $\phi : G \rightarrow \text{Sym}(X)$ defined by $g \mapsto \sigma_g$.

Proposition 3. ϕ is a homomorphism of G to $\text{Sym}(X)$.

Proof. Left for the reader □

A homomorphism $\phi : G \rightarrow \text{Sym}(X)$ is called a **permutation representation** of G associated with G 's action on X . Moreover, that is how we will think about group actions in this course. Given ϕ , $x^g = g \cdot x := \phi(g)x = \sigma_g(x)$.

Similarly, a homomorphism $\psi : G \rightarrow GL(n, \mathbb{F})$ is called a **linear representation** of G . In this case G acts on the corresponding vector space by non-singular linear operators. We will not concentrate on linear representations in this course, but several examples will be considered.

To discuss group action $\phi : G \rightarrow \text{Sym}(X)$ on X further, we need the following definitions.

We call $\ker \phi$ the **kernel of the group action**. It is a normal subgroup of G formed by all elements acting trivially on X , i.e., as the identity map on X .

The action ϕ is called **faithful** if $\ker \phi = \langle e \rangle$. (I would call it ‘not wasteful’.)

For each $x \in X$, the **stabilizer** of x in G is the set $\{g \in G : x^g = x\}$. It is easy to see that the set is a subgroup of G , and it is denoted by G_x . It contains all elements of G which map (move) x to itself. The following proposition is clear.

Proposition 4. $\ker \phi = \bigcap_{x \in X} G_x$

Given G acting on X , consider a binary relation on X defined as $a \sim b$ if there exists $g \in G$ such that $a^g = b$. It is easy to check that \sim is an equivalence relation on X . The equivalence classes of \sim are called **orbits** of the action, or just the orbits of G , if X is understood. They partition X . The orbit containing point $x \in X$ is the set $\{x^g : g \in G\}$, which is often denoted by x^G . For any $S \subset G$, $x^S := \{x^s : s \in S\}$.

Theorem 25. *Let $\gamma : x^G \rightarrow (G : G_x)$ be a map defined as follows: if $a = x^g$, then $a \mapsto G_x g$.*

- (i) *Then γ is well-defined and is a bijection.*
- (ii) *If G is finite, $|x^G| = |G : G_x| = |G|/|G_x|$.*
- (iii) *Stabilizers of two points on the same orbit are conjugate subgroups of G .*

Proof. Let $a = x^g = x^{g'}$. Then $x^{g'g^{-1}} = x \Leftrightarrow g'g^{-1} \in G_x \Leftrightarrow g' \in G_x g$. Hence $G_x g' = G_x g$, which proves that γ is well-defined. This also shows that if two elements of G map x to a , then they are in the same right coset of G_x . Conversely, every two elements from the same right coset of G_x map x to the same point, as $x^{G_x g} = x^g$.

The second statement follows from this bijection.

For the third statement, let x and y be in the same orbit. Then $x^g = y$ for some $g \in G$. Consider a map $f : G_x \rightarrow G_y$, such that $h \mapsto g^{-1}hg$. Then f is an injective group homomorphism (why?). To show that f is surjective, take $b \in G_y$ and consider $a = bgb^{-1}$. Then $x^a = x^{gbg^{-1}} = y^{bg^{-1}} = y^{g^{-1}} = x$. So $a \in G_x$. As $f(a) = b$, the proof is finished. \square

If G acts on X and has only one orbit, then this orbit is X , and we say that G acts **transitively** on X . Hence transitivity means that for every two points of X , there exists an element of G which maps one point to another. It is clear that if G is transitive on a finite set X , then $|X| = |G : G_x|$. Combining Proposition 4 and Theorem 25.(iii), we obtain that if ϕ is a transitive action of G on a finite set X , then the kernel of the action can be expressed as

$$\ker \phi = \bigcap_{g \in G} gG_a g^{-1},$$

where $a \in X$ is a (fixed) point, and $\ker \phi$ is independent of a .

Therefore any action of a group on a set is reduced to the transitive actions on the orbits. In what follows we will see that the latter is equivalent to very particular actions of G arising from the right (left) regular representation of G , which we will also define below.

- Let us first explain what we mean by ‘equivalent’ in this context.

Let $G \leq \text{Sym}(X)$ and $H \leq \text{Sym}(Y)$ be two permutation groups. G and H are called **similar** if there exist an isomorphism $\alpha : G \rightarrow H$ (of abstract groups), and a bijection $\beta : X \rightarrow Y$ such that $\beta(x^g) = \beta(x)^{\alpha(g)}$ for every $x \in X$, and every $g \in G$. Similar permutation groups are isomorphic as abstract groups, but it is easy to construct an example of two permutation groups which are isomorphic as abstract groups, but not similar. Take $\langle (12) \rangle$ acting on $[2]$ and $\langle (12)(34) \rangle$ acting on $[4]$.

- Now we describe the ‘particular’ transitive action.

Let G act on itself by right (left) multiplication, i.e., $X = G$ and any $x \in G$ is mapped by $g \in G$ to xg (gx). Here xg (gx) is the result of the operation of G applied to x and g . The corresponding homomorphism $G \rightarrow \text{Sym}(G)$ is called the **right (left) regular representation** of G . The term **regular** in the context of group actions is used for transitive actions with G_x being trivial for each $x \in X$.

Let $H \leq G$. Then the right multiplication induces an action on the right cosets $(G : H)$ via $Hx \mapsto (Hx)g = H(xg)$.

- (i) Trying to generalize Theorem 25.(iii) to infinite groups, one can arrive to the following question:

Let G be an infinite group, and let $H \leq G$. Is it possible to have $g^{-1}Hg < H$ for some $g \in G$? (The containment is strict!)

It turns out that it is possible. The two examples are described below.

- (i) Let $G = \text{Sym}(\mathbb{Z})$ and let H be a subgroup of G generated by an infinite set of some transpositions of G :

$$H = \langle (12), (23), \dots, (n \ n+1), \dots \rangle.$$

Let $g \in G$ be defined as $x \mapsto x+1$ for all $x \in \mathbb{Z}$. Then $g^{-1}(n \ n+1)g = (n+1 \ n+2)$. Prove that this implies that $g^{-1}Hg < H$.

- (ii) (Optional) Show that group $G \leq GL(2, \mathbb{Q})$ formed by the matrices

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}, \quad (\text{hence } \alpha \neq 0),$$

contains a subgroup H such that $g^{-1}Hg < H$ for some $g \in G$.

Lecture 13.

Let $H \leq G$. Then the right multiplication induces an action on the right cosets $(G : H)$ via $Hx \mapsto (Hx)g = H(xg)$. Consider this action.

Theorem 26. *Let $H \leq G$, and let G act on the set of right cosets $(G : H)$ by right multiplication.*

- (i) *The action is transitive.*
- (ii) *$G_H = H$; (here H in the subscript in G_H is the point $H = He$).*
- (iii) *The kernel of the action is $\bigcap_{g \in G} gHg^{-1}$. This is the maximal normal subgroup of G contained in H .*

Proof. A straightforward verification. Done in the text and in class. □

Theorem 27. *Let G be a transitive action of G on X and $a \in X$. Then the action is similar to the action of G on the set of the right cosets $(G : G_a)$ by right multiplication.*

Proof. Will do in class. □

Therefore one does not have to go through all X in order to study transitive actions of G : they all can be constructed “within” G itself!

The following is the celebrated theorem of A. Cayley. It follows immediately from Theorem 26 if $H = \langle e \rangle$ and The First IT (Isomorphism Theorem).

Theorem 28. (Cayley’s Theorem) *Every group of order n is isomorphic to a subgroup of S_n .* □

As S_n can be generated by two elements, e.g., a transposition and an n -cycle, Cayley’s theorem implies that every finite group is isomorphic to a subgroup of a group with only two generators!

Though Cayley’s theorem implies that the whole theory of finite groups can be reduce to the study of S_n , this is not how the group theory developed. Often it is not the easiest way to proceed, and the notion of abstract group is very beneficial. It allows to discuss groups in ‘coordinate free’ manner. Similar happened in field theory: though every finite extension of a field \mathbb{F} is isomorphic to $\mathbb{F}[x]/(p(x))$, the notion of abstract field simplifies many arguments tremendously.

If you are a fan of $GL(n, \mathbb{F})$, you may get even more excited by the following statement.

Corollary 7. *Every group of order n is isomorphic to a subgroup of $GL(n, \mathbb{F})$.*

Proof. If $\pi \in S_n$, consider a 0 – 1 permutation matrix $P = P(\pi)$ defined in the following way. The (i, j) -entry of P is 1 if $\pi(i) = j$, otherwise it is 0. Then the map $S_n \rightarrow GL(n, \mathbb{F})$ defined by $\pi \mapsto P(\pi)$ is a monomorphism (i.e., injective homomorphism). □

Corollary 8. *If G is a finite group and p is the smallest prime divisor of $|G|$, then any subgroup of G of index p (if such exists) must be normal.*

Proof. Did in class. □

Lecture 14.

Let G be a finite group acting on a finite set X transitively. Then $|X| = |G : G_x|$, for any $x \in X$. This simple fact allows one to compute the order of complete groups of symmetry of geometrical figures, or the orders of complete automorphism groups of graphs.

Let \mathbb{E}^n denote the Euclidean n -dimensional space. An **isometry** f of \mathbb{E}^n is a distance preserving map of \mathbb{E}^n to itself, i.e., a map $f : \mathbb{E}^n \rightarrow \mathbb{E}^n$ such that for any $x, y \in \mathbb{E}^n$, the distance between x and y is equal the distance between $f(x)$ and $f(y)$. One can show that an isometry is a bijection (why is it surjective?). If $\Phi \subseteq \mathbb{E}^n$, then $Sym(\Phi)$, is the set of all isometries of \mathbb{E}^n which map Φ to itself. It is clear that $Sym(\Phi)$ is a group with respect to the composition of maps. We call it the **group of (Euclidean) symmetries** of Φ .

Let $\Gamma = (V, E)$ be a simple graph, with the vertex set $V = V(G)$, and the edge set $E = E(G)$. For a simple graph, E is a subset of 2-subsets of V . Let us denote an edge $\{x, y\}$ also as xy or yx . A bijection $f : V \rightarrow V$ is called an **automorphism** of Γ , if $xy \in E$ if and only if $f(x)f(y) \in E$. The set $\text{Aut}(\Gamma)$ of all automorphisms of Γ forms a group with respect to the composition of maps. We call it the **automorphism group** of Γ .

Let us consider two examples of computation of $|Sym(\Phi)|$ or $|\text{Aut}(\Gamma)|$.

1. Consider a regular n -gon P_n in \mathbb{E}^2 . For any of its two vertices x and y , there exists a rotation around its center by an angle $2\pi m/n$, $m \in \mathbb{Z}$, which maps x to y . Since the rotations are isometries of \mathbb{E}^2 , $G = Sym(P_n)$ acts transitively on the set of all n vertices of P_n . What is $|G|$? Consider G_x . It is easy to argue that the only symmetries of P_n which fix x are the identity map and the reflection with respect to the axis of symmetry of P_n which passes through x . Hence $|G_x| = 2$. As $n = |G|/|G_x|$, we obtain that $|G| = 2n$. In addition to n rotations, there are n reflections with respect to n axis of symmetry of P_n . Hence, we have at least $2n$ symmetries of P_n . As $|G| = 2n$, we conclude there are no others! As we know, G is often denoted by D_{2n} and is called the **dihedral** group.

Thinking about P_n as a graph, a cycle C_n , by a similar argument we get $|\text{Aut}(C_n)| = 2n$. Instead of a rotation by angle $2\pi/n$ we consider a cycle $r = (12 \dots n)$ in the symmetric group of all permutations on $V(C_n) = [n]$. The reflections correspond to permutations s , where s is $(i)(i-1, i+1)(i-2, i+2) \dots$ for n odd, and s is any of the $n/2$ reflections of the type $(i, i+1)(i-1, i+2) \dots$ (the axis do not pass through vertices) and $n/2$ reflections of the type $(i)(i+n/2)(i+1, i+1+n/2) \dots$ (the axis pass through two opposite vertices) for n even, $i \in [n]$; all computations are modulo n . \square

Comment. The above implies that $\text{Aut}(C_n) \cong D_{2n}$ is generated by $\{r, s\}$, where s in any reflection. Indeed, as $\langle r \rangle$ contains no reflection s (why?), $|\langle r, s \rangle| > n$. As $|\langle r, s \rangle| \leq 2n$, $|\langle r, s \rangle| = 2n$.

2. Consider a cube Q_3 in \mathbb{E}^3 . It has many symmetries. For example, there are 3 axes of rotational symmetries, each passing through the centers of opposite faces. Any rotation by angle $\pi n/2$, $n \in \mathbb{Z}$, with respect to any of them is a symmetry.

Let x and y be two vertices of Q_3 . It is clear that by using compositions of two of them, x can be mapped to y . Hence, $G = \text{Sym}(Q_3)$ acts transitively on the set of all 8 vertices of Q_3 . What is $|G|$? Consider G_x . Let y, z, w be three vertices of the cube joined to x . Obviously, $H = G_x$ acts on $\{y, z, w\}$. It is easy to argue (do it!) that this action is also transitive: rotations of \mathbb{E}^3 by angles $2\pi m/3$ with respect to the “long” diagonal of the cube passing through x can map any point of $\{y, z, w\}$ to any other point of this set, and also cube to itself. The action $(G_x, \{y, z, w\})$ is faithful (its kernel is the identity), as the only isometry of \mathbb{E}^3 which fixes four non-coplanar points x, y, z, w must be the identity map. Hence, $3 \leq |G_x| \leq 3! = 6$. Hence, $|G| = 8 |G_x|$, and the problem now is to determine $|G_x|$. For every of these 6 permutations of $\{y, z, w\}$, one can easily find an isometry of \mathbb{E}^3 which realizes it and fixes x . Moreover, any such an isometry will map Q_3 to itself. Hence $|G_x| = 3! = 6$, and $|\text{Sym}(Q_3)| = 8 \cdot 6 = 48$.

If one has difficulties of seeing that $|G_x| = 6$, it is possible to proceed with a few smaller steps. We can do it by using the same logic again! Consider the stabilizer of point y in $(H = G_x, \{y, z, w\})$. $H_y = G_x \cap G_y$ consists of all isometries of \mathbb{E}^3 which fix both x and y . Then H_y acts on $\{z, w\}$. This action is transitive, as z can be mapped to w by the reflection of the plane passing through line xy and the diagonal of the face containing x, z and w , and which passes through x . Note that this reflection also maps the cube to itself. Therefore $|H_y| = 2$, and $|G_x| = 3 |H_y| = 6$. \square

Knowing that $|\text{Sym}(Q_3)| = 48$, one can easily *find all* elements of $\text{Sym}(Q_3)$. First we observe, that some symmetries preserve the orientation of the cube in \mathbb{E}^3 , and some do not.

Let us make the notion of ‘orientation’ more precise. It is easy to see that every isometry of \mathbb{E}^3 which is a symmetry of the cube fixes the center of the cube. Indeed, such a symmetry permutes the vertices of the cube. Hence, as the center of the cube is equidistant from the vertices, so should be its image. As there exists only one point in \mathbb{E}^3 with this property, the center of the cube must be fixed by each its isometry.

Consider now an isometry of \mathbb{E}^3 which fixes the center of the cube (not necessarily its symmetry). Consider the underlying vector space \mathbb{R}^3 or \mathbb{E}^3 , with zero vector corresponding to the center of the cube. One can show that the isometry must be a linear map of the \mathbb{R}^3 (Show this!) The set of all linear maps of \mathbb{R}^3 which preserve the distances form a subgroup in $GL_3(\mathbb{R})$ that is called the **orthogonal group** of \mathbb{R}^3 , and is denoted by $O_3(\mathbb{R})$. Such maps are often referred to as **orthogonal transformations** or **orthogonal maps**. Thus, $\text{Sym}(Q_3) < O_3(\mathbb{R})$. If a basis of \mathbb{R}^3 is chosen, a matrix which corresponds to an orthogonal map is called an **orthogonal matrix**. It is a well known fact that the determinant of an orthogonal matrix is 1 or -1 . (Why?)

Now, the isometries which preserve the orientation correspond to orthogonal maps with determinant 1, and those which do not – to maps with determinant -1 . Those with determinant 1 form a subgroup $O_3^+(\mathbb{R})$ of index 2 in $O_3(\mathbb{R})$. Hence, it is a normal subgroup. Often the elements of $O_3^+(\mathbb{R})$ are referred to as **rotations**, or **rigid motions**, or **proper motions**. They correspond to the ‘mechanical’ motions in 3-space. Similar notions and terminology exists for $O_n(\mathbb{F})$, where $n \geq 1$ and \mathbb{F} is any field of characteristic distinct from 2.

Consider the rotations of Q_3 , i.e., $Sym^+(Q_3) = Sym(Q_3) \cap O_3^+(\mathbb{R})$. There are 24 of them, and they can be all listed without much effort. What can help is realizing that *any* orthogonal map in \mathbb{R}^3 fixes a line (why?), and so, if it is a rigid motion, it is a rotation around the line. This explains the use of the term ‘rotation’. Here they are

All rotations of the cube:

- (i) The identity map.
- (ii) Take a line passing through the centers of opposite faces. There are 3 distinct nontrivial rotations in space around the line mapping the cube to itself: the corresponding angles can be chosen as $\pi/2, \pi, 3\pi/2$. There are three such lines, which give 9 such rotations. It is easy to see that all these rotations are distinct symmetries of the cube. (Why?) This gives 9 distinct symmetries of this type.
- (iii) There are four ‘long’ diagonals of the cube, and rotations around them by angles $2\pi/3$ and $4\pi/3$ give 8 symmetries of the cube. It is clear that they are all distinct (why?), and each distinct from the rigid motions described above.
- (iv) We also can rotate the cube around a line passing through the midpoints of a pair of opposite parallel edges (the ones not in a face) by angle π . As there are six such pairs, there are 6 such rotations. It is easy to see that they are all distinct, and that none of these symmetries coincide with any described above.

As we already obtained $1 + 9 + 8 + 6 = 24$ distinct rotations, there cannot be any others, and so we are done.

Comment. One can also consider a graph, called binary 3-cube. Its vertices are all eight vectors with three components, each component is 0 or 1. Two vertices form an edge if and only if the sequences differ exactly in one component. Let us denote this graph by Q_3^2 . Computation of $|\text{Aut } Q_3^2|$ is similar to $Sym(Q_3)$, where isometries are replaced by permutations of the set of vertices. The groups are isomorphic.

In general, the groups of figures and corresponding graphs *do not* have to be isomorphic. For example, a line segment in \mathbb{E}^3 has infinite symmetry group: any rotation in space around the line containing the segment is in it. But when considered as a graph with 2 vertices and 1 edge, often denoted by K_2 , one obtains $\text{Aut}(K_2) \cong S_2$.

Lecture 15.

Our next application of group actions, is a not-so-easy class of counting problems. Let a group G act on X . For any element $g \in G$, let

$$\chi(g) = |\{x \in X : x^g = x\}|,$$

the number of fixed points of g . We call χ the **permutation character**³ of g .

Theorem 29. (Cauchy-Frobenius) *Let G be a finite group acting on a finite set X , and let $\mathcal{O}_1, \dots, \mathcal{O}_t$ be its all orbits. Then*

$$t = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

Proof. We consider the set $S = \{(x, g); x \in X \text{ and } x^g = x\}$, and count $|S|$ in two ways. For a fixed g , there $\chi(g)$ elements $x \in X$ such that $(x, g) \in S$. Hence

$$|S| = \sum_{g \in G} \chi(g).$$

For a fixed $x \in X$, there exist $|G_x|$ group elements g such that $(x, g) \in S$. Hence

$$|S| = \sum_{x \in X} |G_x| = \sum_{k=1}^t \sum_{x \in \mathcal{O}_k} |G_x| = \sum_{k=1}^t |G_x| \cdot |\mathcal{O}_k| = \sum_{k=1}^t |G| = t|G|.$$

The third equality above is due to the fact that the stabilizers of distinct points of any orbit are conjugate subgroups, and therefore all have same order. Comparison of the two expressions for $|S|$ proves the theorem. \square

Comment. This theorem is also often referred to as Burnside's Lemma. The result is not due to Burnside himself, who merely quotes it in his very influential book "On the Theory of Groups of Finite Order" (1897), attributing it instead to Frobenius (1887). But even prior to Frobenius, the formula was known to Cauchy in 1845. Consequently, this lemma is sometimes referred to as 'Not Burnside's Lemma'.

Here is a famous application of this theorem.

Corollary 9. *Let G be a finite permutation group on a finite set X with at least two elements. Then G contains a permutation without fixed points.*

Proof. As transitive group has only one orbit, namely X , we have

$$1 = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

As $\chi(e) \geq 2$, and the average value of all $\chi(g)$ is 1, there should be at least one permutation $g \in G$ with $\chi(g) < 1$. As $\chi(g)$ is always a nonnegative integer, $\chi(g) = 0$. \square

³The term 'character' is widely used in linear representation of groups where group elements are represented by linear operators, or matrices, when a basis of the space is fixed. The character of an element is the trace of a matrix which represents it. The definition does not depend on a basis of the space. When permutations are represented by the permutation matrices, the trace of such a matrix is precisely the number of fixed points of a permutation. That is why we called this number the 'character' of g .

By a result of Fein, Kantor, and Schacher (1981), every transitive permutation group on at least two points contains a fixed-point-free element of prime power order. Their proof relied on the Classification of Simple Groups.

Let us apply the lemma to the following problem.

Problem 1. *Each face of a 3-dimensional cube can be colored in one of the given n colors. How many different colorings are there?*

Solution. The way the problem is stated is *very* ambiguous. How should one understand the term ‘different’? Or, equivalently, how does one define ‘the same’ colorings? One can suggest various definitions, and the answer may depend on such a definition.

Let us assume that the faces are labeled, and the set F be the set of all six faces. Let $[n]$ represent the set of n colors. A **coloring** of faces is any function $\lambda : F \rightarrow [n]$. Let Λ denote the set of all n^6 colorings of F in colors from $[n]$. Every group G of symmetries of the cube induces two actions: (G, F) and (G, Λ) . The first action is clear. The second action can be defined in the following way: for any $f \in \Lambda$ and any $g \in G$, let f^g be a coloring from Λ such that $f^g(x) = f(x^g)$ for all $x \in F$. We say that two colorings are **G -equivalent**, or **G -same**, if they belong to the same orbit of (G, Λ) . Two colorings which are not G -equivalent, can be called **G -distinct**. Then the problem can be understood as determining the number of orbits of (G, Λ) .

Therefore we have to choose G ourselves. Let G be the set of all 24 rotations of the cube. In order to apply the Cauchy-Frobenius theorem, we have to determine the values of all $\chi(g)$. Using the description of the elements of the group above, we obtain:

- (i) $\chi(e) = n^6$ (all faces are fixed and arbitrarily colored).
- (ii) If g is of type (ii), the faces perpendicular to the axis are fixed. If the rotation is by an angle $\pi/2$ or $3\pi/2$, the remaining four faces must be colored the same. This gives n^3 fixed colorings. If the rotation is by an angle π , the remaining two pairs of opposite faces can be colored the same. This gives n^4 fixed colorings. Hence the total number of fixed colorings for this type of elements is $6 \cdot n^3 + 3 \cdot n^4 = 6n^3 + 3n^4$.
- (iii) If g is of type (iii), it fixes no face, and permutes two groups of three faces in a cyclic order. Choosing a color for each triple, gives n^2 colorings. Hence the total number of fixed colorings for this type of elements is $8 \cdot n^2$.
- (iv) If g is of type (iv), no face is fixed, and each pair of opposite faces can be assigned a color arbitrarily. Hence the total number of fixed colorings for this type of elements is $6 \cdot n^3$.

Therefore, the number t of orbits of (G, Λ) is

$$t = \frac{1}{24} (n^6 + 3n^4 + 12n^3 + 8n^2).$$

More examples of this type of counting were distributed in class.

Lecture 16.

We remind the reader that $y \in G$ is called **conjugate to** $x \in G$ if $y = g^{-1}xg$ for some $g \in G$. It is easy to see that the conjugacy is an equivalence relation on G . The equivalence classes are called the **conjugacy classes of G** and they partition G .

Another important action of G on itself ($X = G$) is **the action by conjugation**, when $g \in G$ acts on G via $x \mapsto g^{-1}xg$ for all $x \in G$. It is easy to see that this definition indeed gives an action of G . Moreover, for each $g \in G$, the mapping is an automorphism of G , even if G is infinite. This is not the case for regular representations of G , where only the identity produces an automorphism, since any $g \neq e$ maps e to $eg = g$. Another distinction is that the action by conjugation is never transitive (unless G is trivial): $\{e\}$ is always an orbit.

Orbits of the action of G on G by conjugation are exactly the conjugacy classes of G . As, for any action, x^G denotes the orbit of x ,

$$G = \bigcup_{x \in G} x^G = \bigcup_{x \in G} (\text{conjugate class containing } x).$$

An important example of conjugation appears in linear algebra, where $GL(n, \mathbb{F})$ acts on the ring of all $n \times n$ matrices over \mathbb{F} , and, in particular, on itself, by conjugation.

With every action of G on a set X , we have an induced action of G on 2^X , where for $A \subseteq X$, $A^g = g \cdot A := \{a^g = g \cdot a : a \in A\}$.

If A and B are two subsets of G and $B = g^{-1}Ag$ for some $g \in G$, then A and B are called **conjugate in G** . In other words, two subsets conjugate in G lie on the same orbit in the induced action of G (by conjugation) on 2^G .

Let $A \subseteq G$. Then the set $\{g \in G : g^{-1}Ag = A\}$ can be viewed from two different perspectives. On the one hand it describes the set of all elements of G for which $gA = Ag$, where A does not have to be a subgroup. Then it is called the **normalizer of A in G** and is denoted by $N_G(A)$. On the other hand, the set represents the stabilizer of a point A in the induced action of G (by conjugation) on 2^G . Then it has to be denoted by G_A , as we did for the stabilizer of a point $x \in X$ when G acted on X . No matter how we view it, the set is a subgroup in G . Therefore we have

$$G_A = N_G(A) := \{g \in G : g^{-1}Ag = A\}.$$

Another notion which proved useful in group theory is of the **centralizer subgroup of $A \subseteq G$** , which is denoted by $C_G(A)$ or by $Z_G(A)$, and is defined as

$$C_G(A) = \{g \in G : ag = ga \text{ for all } a \in A\}.$$

It is clear that

$$\langle e \rangle \leq C_G(A) \leq N_G(A) \leq G,$$

$$C_G(A) = \bigcap_{a \in A} N_G(\{a\}),$$

since $C_G(\{a\}) = N_G(\{a\})$ for each $a \in A$.

For those who remember Theorem 25, the following proposition must be trivial.

Proposition 5. *Let G act on itself by conjugation, and $A \subseteq G$. Then the number of subsets B of G conjugate to A is $|G : N_G(A)| = |G : G_A|$.*

If $A = G$, $C_G(G)$ is called the **center of G** and is denoted by $Z(G)$. In other words, the center of a group G is the set of all its elements that commute with every element of G . It is clear that $Z(G) \neq G$, and $Z(G) = G$ if and only if G is abelian. Often, when one think about finding a normal subgroup in an non-abelian group, one searches for its center, or for its commutator subgroup.⁴

To those who suffered through all these definitions, the following fundamental theorem is a reward.

Theorem 30. (The Class Equation) *Let G be a finite group and let g_1, g_2, \dots, g_r be representatives of all conjugacy classes of G not contained in the center of G . Then*

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|.$$

Proof. Discussed in the text and in class. □

The following is a very important corollary.

Corollary 10. *If G is a finite group of order p^a , p is prime, $a \geq 1$, then it has a non-trivial center. If such a group is non-abelian, then it is not simple.*

Proof. Done in the text and in class. It is also clear that if such a group is abelian, then it is simple only if $a = 1$. □

Corollary 11. *If G is a finite group of order p^2 , p is prime, then G is abelian and is isomorphic to C_{p^2} or $C_p \times C_p$.*

Proof. Done in the text and in class. In our proof the following useful lemma were used.

Lemma 2. *If the factor group $G/Z(G)$ is cyclic, then G is abelian.*

Make sure you can prove this lemma. □

Problems.

- (i) What is the center of D_{2n} , and how many conjugacy classes does it have?
- (ii) What is the center of S_n , and how many conjugacy classes does it have? For the second question, answer it for $n = 8$, and find a recurrence formula for the general case. Do not look for an explicit formula. Find (look somewhere) information about the asymptotics of this number for $n \rightarrow \infty$.
- (iii) What is the center of A_n ?
- (iv) What is the center of $GL(n, \mathbb{F})$?
- (v) How many conjugacy classes does $GL(2, \mathbb{F}_q)$ have?
- (vi) Find all finite groups which have exactly two conjugacy classes.

⁴The **commutator subgroup** of G , often denoted by G' , is the minimal subgroup of G such that G/G' is abelian. One can show that G' is generated by the commutators $[g_1, g_2] = g_1^{-1}g_2^{-1}g_1g_2$ of every two elements g_1 and g_2 of G .

Lecture 17.

By Lagrange's Theorem, the order of a subgroup of a finite group G divides $|G|$. The converse, namely that for every divisor k of $|G|$, there exists a subgroup of G of order k is not true in general. For example, A_4 of order 12 has no subgroup of order 6. (Why?)

The following theorem is fundamental in the theory of finite groups. Let G be a group, and let p be a prime. A group of order p^a , $a \in \mathbb{N}$, is called a **p -group**. A subgroup H of G is called a **p -subgroup** if H is a p -group. If p^a divides $|G|$, but p^{a+1} does not, a subgroup of G of order p^a is called a **Sylow p -subgroup** of G . The set of Sylow p -subgroups of G is denoted by $Syl_p(G)$, and the number of Sylow p -subgroups of G is denoted by $n_p(G)$ or just n_p . Hence, $|Syl_p(G)| = n_p(G)$.

The theorem below is a generalization of the results of Sylow (1872).

Theorem 31. (Sylow's Theorem) *Let G be a group of order $p^k m$, where p is a prime. Then the following holds.*

- (i) *The number of subgroups of G of order p^k is congruent to 1 modulo p . In particular, G contains a subgroup of order p^k .*
- (ii) *Every p -subgroup of G is contained in some Sylow p -subgroup of G .*
- (iii) *All Sylow p -subgroup of G are conjugate.*
- (iv) *If p^{k+1} divides $|G|$, then every subgroup of G of order p^k is contained in a subgroup of G of order p^{k+1} .*
- (v) *if p does not divide m , n_p divides m .*

Proof. (i) Let $S = \{A : A \subseteq G \text{ and } |A| = p^k\}$. Consider the regular action (G, G) , where $x \mapsto xg$. This action induces an action (G, S) , where $A \mapsto Ag$. Let G_A be the stabilizer of A in G . Then G_A acts on A .

What are the orbits of this action (G_A, A) ? Note that for each $a \in A$, $aG_A \subseteq A$ (since G_A acts on A). Hence, the orbits are the left cosets aG_A of G_A in G , with $a \in A$, and A is partitioned into these left cosets. This implies that

$$|G_A| \text{ divides } |A| = p^k, \text{ and so } |G_A| = p^a, \text{ where } 0 \leq a \leq k. \quad (0.3)$$

Let $S_k = \{A : A \in S \text{ and } |G_A| = p^k\}$, and, due to (0.3),

$$\overline{S_k} = S \setminus S_k = \{B : B \in S \text{ and } |G_B| = p^a, \text{ with } 0 \leq a < k\}.$$

For every $B \in \overline{S_k}$, the length of the orbit it belongs to in the action (G, S) is $|B^G| = |G|/|G_B|$, and so it is divisible by pm . Hence,

$$|S| \equiv |S_k| \pmod{pm}. \quad (0.4)$$

Now we prove that S_k is partitioned into all left cosets of all subgroups of G containing p^k elements.

Indeed, as we have concluded above, for every $A \in S$, and every $a \in A$, $aG_A \subseteq A$. Hence, $|aG_A| = |G_A| \leq |A|$. For $A \in S_k$, this gives $aG_A = A$. Hence S_k consists only of the left cosets of a subgroup of G with p^k elements, maybe not all.

Conversely, let $H \leq G$, and $|H| = p^k$, and let xH be *any* of its left cosets. Then $|xH| = |H| = p^k$, and so $xH \in S$. As $(xH)H = xH$, we have that $H \subseteq G_{xH}$ – the stabilizer of xH in G (for the action (G, S)). Hence, $p^k \leq |G_{xH}|$. As $|G_H| \leq p^k$ from (0.3), we conclude that $|G_H| = p^k$, $G_{xH} = H$, and $xH \in S_k$.

Therefore S_k consists of all left cosets of all subgroups of G of order p^k , or empty, if such do not exist. Let H_1 and H_2 be two distinct subgroups of G of order p^k . Then no coset of H_1 is equal to a coset of H_2 (why?). Therefore, if n denotes the number of subgroups of G having p^k elements, then we have

$$|S_k| = nm. \quad (0.5)$$

Note that $|S|$ depends only on $|G|$ and p^k (actually it is equal to $\binom{|G|}{p^k}$). By (0.4) and (0.5),

$$n = \frac{|S_k|}{m} \equiv |S| \pmod{p}.$$

Indeed, $|S| - |S_k| = |S| - mn = t(pm)$ for some integer t . Hence, $|S| = mq$, for some integer q , and $|S| - |S_k| = m(q - n) = t(pm)$ gives $q - n = tp$.

Therefore the congruence class $n \pmod{p}$ depends only on $|G|$ and p^k , but not on G ! Taking G to be a *cyclic* (!) group of order $p^k m$, we obtain that for this group $n = 1$, as it contains exactly one subgroup for each divisor of its order. Hence, $n \equiv 1 \pmod{p}$ for each G of order $p^k m$, and the proof of this part of the theorem is finished. \square

(ii) Let H be a p -subgroup of G , and let P be a Sylow p -subgroup of G (it exists by part (i)). Consider an action of H on $(G : P)$ by $Pg \mapsto P(gh)$ for $h \in H$. Since the number of elements in any orbit of this action is the index of the stabilizer of a point of the orbit in H , the length of any orbit is 1 or a power of p greater than 1. Hence, it is 1 or it is divisible by p . The sum of lengths of all orbits is $|(G : P)|$, and so it is not divisible by p . Therefore there exists an orbit of length 1, which is formed by a fixed point of this action. Let a fixed point be Pg . Then $Pg = P(gh)$ for all $h \in H$, and so $H \subseteq g^{-1}Pg$ (why?). As a conjugation of G is an automorphism of G , then $g^{-1}Pg$ a subgroup of G isomorphic to P , and so it is a p -Sylow subgroup of G . This shows that H is a subgroup of a Sylow p -subgroup of G , and proves part (ii). \square

(iii) This follows immediately from our argument for part (ii). If H is a Sylow p -subgroup, then, comparing the orders, we get $H = g^{-1}Pg$. This shows that every Sylow p -subgroup of G is conjugate to P , and therefore all Sylow p -subgroups of G are conjugate. \square

(iv) Let p^{k+1} divide $|G|$, and let H be a subgroup of G of order p^k . By part (ii), we know that H is a subgroup of a Sylow p -subgroup of G , call it P . Consider an action of H on $(P : H)$ by $Hg \mapsto H(gh)$ for $h \in H$. Since the number of elements in any orbit of this action is the index of the stabilizer of a point of the orbit in H , the length of any orbit is 1 or a power of p greater than 1. Hence, it is 1 or it is divisible by p . The sum of lengths of all orbits is $|(P : H)|$, and so it is divisible by p . As $H = He$ is a fixed point of this action, there must be another fixed point (actually, at least $p - 1$ other fixed points). Let it be Hg , $g \in P \setminus H$. Then $Hg = H(gh)$ for

all $h \in H$, and so $H \subseteq g^{-1}Hg$. Comparing the orders, we get $H = g^{-1}Hg$. As $g \notin H$, we get $H \triangleleft N_P(H)$ and $H \neq N_P(H)$. Since $N_P(H) \leq P$, then $N_P(H)$ is a p -group, and, hence, $N_P(H)/H$ is p -groups. By (i), $N_P(H)/H$ contains a subgroup of order p , which, by the Fundamental Isomorphism Theorem, is K/H , for some subgroup K of $N_P(H)$, $H \triangleleft K \leq N_P(H)$. As $|K| = p^{k+1}$, the proof of part (iv) is finished. \square

(v) Let P be a Sylow p -subgroup of order p^k . Then $m = |G : P|$. As all Sylow p -subgroups are conjugate in G , the action of G on the set of all of them by conjugation has only one orbit, and the length of the orbit is n_p . The stabilizer of this action is $N_G(P)$, hence $n_p = |G : N_G(P)|$. As $P \leq N_G(P) \leq G$, we have $n_p = |G : N_G(P)|$ divides $|G : P| = m$. This proves part (v). \square

We state the intermediate results obtained in our proof of parts (i) and (ii) as corollaries.

Corollary 12. (i) For a prime positive integer p , $\frac{1}{m} \binom{p^k m}{p^k} \equiv 1 \pmod{p}$.

(ii) If H is a p -subgroup of G , P be a Sylow p -subgroup of G , then $H \text{ lineqq } N_P(H) \leq N_G(H)$.

(iii) P is the unique Sylow p -subgroup, i.e., $n_p = 1$.

Comments.

- (i) Proof of part (i) of Theorem 31 presented in class follows the one by Gallaher (1967). A similar one was suggested much before by G.A Miller (1915), and rediscovered by H. Wieland (1959).
- (ii) The fact that for every prime p which divides the order of G , there exists a subgroup of order p is known as Cauchy's Theorem.
- (iii) For finite *abelian* groups we have a much stronger result: for every divisor m of $|G|$, there exists a subgroup of order m . It is easy to show that every finite abelian group is either a p -group for some prime p , or every Sylow p -subgroup of G is unique, and G is the direct product of its Sylow p -subgroups.

One may wonder whether there exist non-abelian groups sharing some of the properties of abelian groups described in Comment (iii). The answer is YES. A proof of the following theorem are easy to find in the literature (e.g., see Dummit and Foote, or Isaacs texts). Some parts are easy to prove.

Theorem 32. For a finite group G the following statements are equivalent.

- (i) For any $H < G$, $H < N_G(H)$.
- (ii) Every maximal subgroup of G is normal.
- (iii) Every Sylow subgroup of G is normal.
- (iv) Every Sylow p -subgroup of G is unique.
- (v) G is direct product of its Sylow subgroups.
- (vi) All subgroups of G generated by elements of p -power order are p -groups.

Any finite group G satisfying any of the five properties of Theorem 32 is called a **nilpotent** group. The class of nilpotent groups extends the class of abelian groups, and often they are called ‘almost abelian’. It can be shown that in a finite nilpotent group, any two elements of relatively prime orders must commute. Examples: the dihedral group D_4 , the quaternion group Q_8 , and, moreover, every p group is nilpotent. It is easy to argue that every subgroup and every factor group of a nilpotent group is nilpotent, and that the direct product of finitely many nilpotent groups is nilpotent. The definition of an infinite nilpotent group is different, but it is equivalent to ours for finite groups. See the web for the explanation of the term ‘nilpotent’.

Lecture 18.

Here we consider several applications of Sylow theorems.

Problem 2. Describe all isomorphism classes of groups of order 45.

Solution. We show that every group G of order 45 is a direct product of its abelian Sylow subgroups. As $45 = 3^2 \cdot 5$, this will give that there are only two isomorphism classes of such groups:

$$\mathbb{Z}_{45} \cong \mathbb{Z}_9 \times \mathbb{Z}_5 \quad \text{or} \quad \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5.$$

Indeed, by Theorem 31, $n_3 \equiv 1 \pmod{3}$ and $n_3 | 5$. Hence, $n_3 = 1$. Similarly, $n_5 \equiv 1 \pmod{5}$ and $n_5 | 5$. Hence, $n_5 = 1$. Therefore $Syl_3(G)$ and $Syl_5(G)$ are both normal in G , and $Syl_3(G) Syl_5(G) \trianglelefteq G$. Also, every element in $Syl_3(G) \cap Syl_5(G)$ has order dividing 9 and 5, and so the intersection is $\langle e \rangle$. As

$$|Syl_3(G) Syl_5(G)| = \frac{|Syl_3(G)| \cdot |Syl_5(G)|}{|Syl_3(G) \cap Syl_5(G)|} = \frac{45}{1} = 45,$$

G is the direct product of $Syl_3(G)$ and $Syl_5(G)$. Clearly, $Syl_5(G) \cong \mathbb{Z}_5$. We also know that there are two nonisomorphic groups of order p^2 for every prime p , both abelian. Applying this for $p = 3$, we get the result. \square

Problem 3. Describe all isomorphism classes of groups of order pq , where p, q are positive primes, and $p < q$.

Solution. By Theorem 31, $n_q = 1 + tq$ and $n_q | p$. Hence, $n_q = 1$, and there exists a unique Sylow q -group which is normal in G . As its order is q , it is cyclic. Let $B = \langle b \rangle$, $b^q = e$, be this subgroup.

Similarly, $n_p = 1 + tp$ and it divides q . Hence, $n_p = 1$ or q . If it is equal 1, we obtain the only Sylow p -subgroup of order p . So it is normal and cyclic, and in this case, G is the direct product of its Sylow subgroups and is cyclic of order pq .

Now we assume that $n_p = q$, which implies that $p | (q - 1)$. Let $A = \langle a \rangle$, $a^p = e$, be one of Sylow p -subgroups. Since $n_p > 1$, A is not normal in G . As $B \triangleleft G$, we have $AB \leq G$. Any common element of A and B has order dividing both p and q , and so $A \cap B = \langle e \rangle$. Therefore $|AB| = |A| \cdot |B| / |A \cap B| = pq/1 = pq$.⁵ This gives that $G = AB$, and every element of G can be written as $a^i b^j$, $0 \leq i \leq p - 1$, $0 \leq j \leq q - 1$. The information about G that we have obtained, is valuable, but far from satisfactory. In order to understand the structure of G , we have to understand how elements of the form $a^i b^j$ are multiplied.

As B is normal in G , $a^{-1}ba = b^r$ for some r . Then $a^{-1}b^i a = b^{ir}$ for any i , and, in particular, $a^{-1}b^r a = b^{r^2}$. This implies that $a^{-2}ba^2 = a^{-1}b^r a = b^{r^2}$, and, in general, $a^{-j}ba^j = b^{r^j}$. Hence, for $j = p$, we get $b = a^{-p}ba^p = b^{r^p}$. This gives

$$r^p \equiv 1 \pmod{q},$$

as b is an element of order q . We will see that this necessary condition on r leads to a group operation on G . Suppose it is satisfied. The relation $a^{-1}ba = b^r$, implies the following multiplication rule (check!):

⁵Using the equality $|AB| = |A| \cdot |B| / |A \cap B|$ both here and in Problem 2 is, of course, an overkill. If $|G| = pq$, q being prime, and $A < AB \leq G$ implies that $AB = G$.

$$(a^u b^v)(a^x b^y) = a^{u+x} b^{vr^x+y}.$$

In the discussion and the definition above exponents of a and b are, of course, considered by modulo p and q , respectively. If $r \equiv r' \pmod{q}$ and $x \equiv x' \pmod{p}$, then $r'^{x'} \equiv r^x \pmod{q}$, due to the fact that $r^p \equiv 1 \pmod{q}$. Therefore, for $r \in \mathbb{Z}_q$ and $x \in \mathbb{Z}_p$, $r^x \in \mathbb{Z}_q$ is well defined. This suggests the following equivalent description of group elements and the group operation. Consider the Cartesian product $\mathbb{Z}_p \times \mathbb{Z}_q$, where each factor is viewed as additive group. Fix an element r of order p in the multiplicative group of the ring \mathbb{Z}_q , and define the product of (u, v) and (x, y) from $\mathbb{Z}_p \times \mathbb{Z}_q$ as

$$(u, v)(x, y) = (u + x, vr^x + y).$$

The product vr^x is understood as the product in \mathbb{Z}_q . It is easy to check that this operation on $\mathbb{Z}_p \times \mathbb{Z}_q$ is associative, $(0, 0)$ is the identity, and $(-u, -vr^{-u})$ is the inverse of (u, v) . Check! Hence, G is isomorphic to a group $\mathbb{Z}_p \times \mathbb{Z}_q$ with operation defined as above.

If $r = 1$, we get that G is abelian, and, as shown before, is cyclic of order pq .

Let $r \neq 1$. What is left is to realize that there may be different r such that $r^p \equiv 1 \pmod{q}$, and so the multiplication they define may possibly lead to nonisomorphic groups. Let us explain that this is not the case, by showing that if $s \in \mathbb{Z}_q$, $s^p \equiv r^p \equiv 1 \pmod{q}$, then the groups with operations

$$(u, v)(x, y) = (u + x, vr^x + y) \quad \text{and} \quad (u, v)(x, y) = (u + x, vs^x + y)$$

are isomorphic. Let us denote the first group by G_r , and the second by G_s .

It is clear that r in \mathbb{Z}_q generates multiplicative cyclic subgroup of order p in \mathbb{Z}_q^* . As every nonidentity element of this cyclic group generates it, there exist integer $a \not\equiv 0 \pmod{p}$ (or $a \in \mathbb{Z}_p^*$), such that $s^a = r$. For any such a , let

$$f_a : G_r \rightarrow G_s, \quad (u, v) \mapsto (au, v).$$

It is obvious that f is injective, hence, it is bijective. As

$$f_a((u, v)(x, y)) = f_a((u + x, vr^x + y)) = (a(u + x), vr^x + y),$$

and

$$\begin{aligned} f_a((au, v))f_a((ax, y)) &= (au, v)(ax, y) = (au + ax, vs^{ax} + y) = \\ &= (a(u + x), v(s^a)^x + y) = (a(u + x), vr^x + y), \end{aligned}$$

the map f is a group homomorphism. Hence, f_a is an isomorphism.

Summarizing our findings, we have the following complete description of all isomorphism classes of groups of order pq , where p, q are primes, and $p < q$.

For primes p, q , $p < q$,

- if $p \nmid (q - 1)$, then the only group of order pq is the cyclic one.
- if $p \mid (q - 1)$, then there are two isomorphism classes of groups of order pq : the cyclic group, and a nonabelian group. The nonabelian group is isomorphic to the group whose elements are from $\mathbb{Z}_p \times \mathbb{Z}_q$ with operation defined by the rule

$$(u, v)(x, y) = (u + x, vr^x + y),$$

where r is any integer satisfying the condition $r^p \equiv 1 \pmod{q}$. \square

Lecture 19.

Direct products.

For arbitrary groups A and B their **external direct product** is the group on the set $\{(a, b) : a \in A, b \in B\}$, with the operation defined as

$$(a, b)(a', b') = (aa', bb').$$

This group is denoted by $A \times B$ (like the Cartesian product of sets A and B). By now, this notion must be well familiar to the reader.

Let $A, B \trianglelefteq G$, $AB = G$, and $A \cap B = \langle e \rangle$. Then G is called the **internal direct product** of A and B .

It is easy to show that

if G is the internal direct product of its subgroups A and B , then G is isomorphic to the external direct product of A and B .

In order to see it, we first observe that if G is the internal direct product of A and B , then every element of G is represented *uniquely* as ab , where $a \in A$ and $b \in B$. Why? From the definition of the internal direct product, at least one such representation exists. If $ab = a'b'$, with $a, a' \in A$ and $b, b' \in B$, then $a'^{-1}a = bb'^{-1} \in A \cap B = \langle e \rangle$. Hence, $a = a'$, $b = b'$, and the representation is unique. Looking closer to the multiplication in G , we can also conclude something else: every two elements $a \in A$ and $b \in B$ commute! Indeed, $ab = ba \Leftrightarrow (aba^{-1})b^{-1} = e$. As B is normal in G , we get $aba^{-1} = x \in B$. Hence $xb^{-1} = e \Leftrightarrow x = b$. This gives $ab = ba$.

Now consider a map $f : G = AB \rightarrow A \times B$ defined as $f(ab) = (a, b)$. Since every element of G can be written as ab , $a \in A$, $b \in B$, uniquely, the map is well-defined, and is a bijection. We wish to show that f is an isomorphism. Let $g = ab$ and $g' = a'b'$. Then $gg' = (ab)(a'b') = a(ba')b' = a(a'b)b' = (aa')(bb')$, and $f(gg') = f(g)f(g')$ follows. Hence $G \cong A \times B$.

The converse of this statement is true in the following sense. Let $G = A \times B$ be the external direct product of A and B . Then G is an internal direct product of its subgroups $G_A = \{(a, e_B) : a \in A\} \cong A$ and $G_B = \{(e_A, b) : b \in B\} \cong B$. In general, one can form an external direct product of two groups which share a common subgroup distinct from $\langle e \rangle$.

Examples of direct products.

- $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if $(m, n) = 1$.
- $D_{4n} \cong D_{2n} \times \mathbb{Z}_2$.
- Let $I \cup J = [n]$ be a partition of $[n]$, and let $G = \{\sigma \in S_n : I^\sigma = I \text{ and } J^\sigma = J\}$.
Then $G \cong S_{|I|} \times S_{|J|}$.
- $\mathbb{C}^* = \mathbb{R}_+^* \times U$: every nonzero complex number can be uniquely represented in the trigonometric form. Here \mathbb{R}_+^* is the multiplicative group of positive reals, and U is the multiplicative group of complex numbers of norm 1.

- $GL^+(n, \mathbb{R}) = \{\lambda I_n : \lambda > 0\} \times SL(n, \mathbb{R})$, where $GL^+(n, \mathbb{R})$ is the group of matrices with positive determinant.

Semidirect products

Similarly to the notion of the external (internal) direct product of two groups (subgroups), one can consider its broad generalization: the notions of the external (internal) semidirect product of two groups (subgroups).

Let N and B be groups, and let B act on N by automorphisms of A . This means that we have a homomorphism $f : B \rightarrow \text{Aut}(N)$, and $b \in B$ acts on N by $x \mapsto (f(b))(x) = x^{f(b)}$.

Now consider the set $N \times B$ with a binary operation defined as follows: for $(a, b), (x, y) \in N \times B$,

$$(a, b)(x, y) = (ax^{f(b)}, by).$$

It is easy to check that $N \times B$ with this operation is a group. Check it!!! Since the product of two automorphisms is their composition, when we use the exponential notation we must agree that $(g^\alpha)^\beta = g^{\beta\alpha}$. This groups is called the **external semidirect product of N and B with respect to f** , and it is denoted by

$$N \rtimes_f B.$$

It is also easy to check that

$$N \cong \{(a, e_B) : a \in N\} \trianglelefteq N \rtimes_f B, \quad \text{and} \quad B \cong \{(e_N, b) : b \in B\} \leq N \rtimes_f B.$$

If f is a trivial homomorphism, i.e., $f(b) = e_{\text{Aut}(N)} = \text{id}_N$ for all $b \in B$, $N \rtimes_f B \cong N \times B$ – the external direct product of groups N and B .

Now we introduce the internal semidirect product of N and B .

Let $N \trianglelefteq G$ and $B \leq G$, $NB = G$ and $N \cap B = \langle e \rangle$. Then G is called the **internal semidirect product** of N and B , or just the semidirect product, and we write

$$G = N \rtimes B.$$

To reconcile this definition with the one of the external semidirect product, we notice that B acts on N by conjugations, which are automorphisms of N . Let $f : B \rightarrow \text{Aut}(N)$ be defined as $b \mapsto f(b) = \text{conj}(b)$, where $\text{conj}(b)$ is the automorphism of N with respect to the conjugation of N by b : $\text{conj}(b) : a \mapsto b^{-1}ab$. Then it is easy to check that $G \cong N \rtimes_f B$. So if we just use the notation $G = N \rtimes B$, we presume we deal with the internal direct product and that B acts on N by conjugation.

Note that the information that a group G splits into a semidirect product of its normal subgroup N and a subgroup B allows one to represent elements of G as ab , where $a \in N$ and $b \in B$. This representation, generally is not unique, and does not show how the elements of G are multiplied. Hence, it is much less informative compared to the case when G is an internal direct product of its subgroups.

It is easy to see that if $G = N \rtimes B$, then $G/N \cong B$. Check it! Therefore semidirect products provide some solutions to the so-called **group extension** problem:

Given two groups A and B , construct a group G which contain a normal subgroup $N \cong A$ such that $G/N \cong B$.

On the other hand, it would be a mistake to think that for any normal subgroup N of a group G , there exists a subgroup B of G such that $G = N \rtimes B$. For example, for $G = \mathbb{Z}$ and $N = 2\mathbb{Z} \triangleleft G$, there is no such B . (Why?)

Examples of semidirect products.

- Both \mathbb{Z}_6 and S_3 are isomorphic to semidirect products of $N = \mathbb{Z}_3$ and $B = \mathbb{Z}_2$. One can also say that each of them splits into semidirect product of groups isomorphic to $N = \mathbb{Z}_3$ and $B = \mathbb{Z}_2$.

It is clear that $|\text{Aut}(\mathbb{Z}_3)| = 2$. So it is isomorphic to \mathbb{Z}_2 , and there are only two homomorphisms $f : B = \mathbb{Z}_2 \rightarrow \text{Aut}(N) \cong \mathbb{Z}_2$: the trivial one, or the identity. The first homomorphism f_1 makes B act on N by the trivial automorphism of N , i.e., by the identity map on N . The second homomorphism f_2 corresponds to the mapping of each element of N to its inverse (this map is an automorphism of order 2, since N is abelian). Hence $\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_3 \rtimes_{f_1} \mathbb{Z}_2$, and $S_3 \cong \mathbb{Z}_3 \rtimes_{f_2} \mathbb{Z}_2$.

- $S_n = A_n \rtimes \langle (12) \rangle$.
- $S_4 = \text{Kl}_4 \rtimes S_3$, where Kl_4 is the Klein group of order 4, and S_3 is embedded in S_4 as the stabilizer of point 4.
- $GL(n, \mathbb{F}) = SL(n, \mathbb{F}) \rtimes \{\text{diag}(\lambda, 1, \dots, 1) : \lambda \in \mathbb{F}^*\}$.
- In Problem 3 (see previous lecture), we proved that every nonabelian group G of order pq , with p, q prime and $p < q$, splits⁶ into a semidirect product of its subgroups $B = \langle b \rangle \cong \mathbb{Z}_q$ and $A = \langle a \rangle \cong \mathbb{Z}_p$:

$$G = B \rtimes_f A \cong \mathbb{Z}_q \rtimes_f \mathbb{Z}_p,$$

where f can be thought as a conjugation of B by a which raises elements of B to the r -th power: $a^{-1}b^i a = b^{ir} = (b^i)^r$, with $r^p \equiv 1 \pmod{q}$. Also, since $\text{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_q^*$ is the cyclic group of order $q - 1$, the homomorphism $f : \mathbb{Z}_p \rightarrow \text{Aut}(\mathbb{Z}_q)$ is completely defined by the image of the generator of \mathbb{Z}_p . For nontrivial f it must be any element of \mathbb{Z}_q^* of the multiplicative order p , i.e., any generator of the multiplicative subgroup of \mathbb{Z}_q^* of order p . If cyclic groups \mathbb{Z}_p and \mathbb{Z}_q employ additive notations, then its automorphisms correspond to multiplying all elements by a nonzero integer having order p in the group. This correspond to writing $vr^x + y$ in the second component. We have seen that the isomorphism class of G does not depend on the choice of such a generator.

The groups which are semidirect products $\mathbb{Z}_n \rtimes_f \mathbb{Z}_m$, with m, n not necessarily prime, are constructed in similar ways. Here $|\mathbb{Z}_n^*| = \phi(n)$. If $\phi(n)$ is relatively prime with m , the semidirect product will be the direct

⁶The set of elements there was $B \times N$ rather than $N \times B$.

product of N and B . Since \mathbb{Z}_n^* does not have to be cyclic, one has to analyze $\text{Aut}(\mathbb{Z}_n^*)$ and all homomorphisms $f : B \rightarrow \text{Aut}(\mathbb{Z}_n^*)$ more carefully.

- $D_{2n} \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$. The conjugation here is the same as sending every element of \mathbb{Z}_n to its inverse: if s is a symmetry and r is the rotation, then $s^{-1}rs = r^{-1}$.
- For $A \in GL(n, \mathbb{F})$ and $b \in \mathbb{F}^n$, let $\pi(A, b) : \mathbb{F}^n \rightarrow \mathbb{F}^n$ be defined via: $x \mapsto xA + b$ (x is a row vector). Let $AGL(n, \mathbb{F}) = \langle \pi(A, b) : A \in GL(n, \mathbb{F}), b \in \mathbb{F}^n \rangle$, where the operation is understood as the composition of maps. Then $AGL(n, \mathbb{F})$ is a group, and it is called the **group of affine transformations of \mathbb{F}^n** . It is easy to show that $AGL(n, \mathbb{F}) \cong \mathbb{F}^n \rtimes GL(n, \mathbb{F})$, where $M \in GL(n, \mathbb{F})$ acts on \mathbb{F}^n via $x \mapsto xM$.
- Let $\Gamma(n, \mathbb{F})$ be the group of all **semi-linear** operators on a vector space $V = \mathbb{F}^n$, which is defined as follows: for every $A \in GL(n, \mathbb{F})$ and every $\phi \in \text{Aut}(\mathbb{F})$, let $[\phi, A] : V \rightarrow V$, via $x \mapsto Ax^\phi$, where $x^\phi = (x_1^\phi, \dots, x_n^\phi)$.

Then the group $\Gamma(n, \mathbb{F}) \cong GL(n, \mathbb{F}) \rtimes \text{Aut}(\mathbb{F})$ with respect to the action of $\psi \in \text{Aut}(\mathbb{F})$ on $M \in GL(n, \mathbb{F})$ given by $M \mapsto M^\psi$. Semi-linear operators can be thought also as functions $f = f_\phi : V \rightarrow V$ such that $f(x + y) = f(x) + f(y)$ for all $x, y \in V$, and $f(\lambda x) = \lambda^\phi f(x)$ for all $x \in V$ and all $\lambda \in \mathbb{F}$.

- Consider the usual action of $G = GL(n, \mathbb{F})$ on $\mathbb{F}^n \setminus \{0\}$ by $x \mapsto Ax$. Then the stabilizer G_x of a point x is isomorphic to $\mathbb{F}^{n-1} \rtimes GL(n-1, \mathbb{F})$, where $M \in GL(n-1, \mathbb{F})$ acts on \mathbb{F}^{n-1} via $y \mapsto yM$. Hence it is isomorphic to $AGL(n, \mathbb{F})$.
- Let A be a group, and let $B \leq \text{Aut}(A)$. Let $id : B \rightarrow \text{Aut}(A)$ be the identity map. Then action of $b \in B$ on A can be thought as simply as applying the automorphism b . The group $A \rtimes_{id} B$ is also called in this case the **extension of A by a group up of its automorphisms B** . When $B = \text{Aut}(A)$, such extension is called the **holomorph** of A , and it is denoted by $\text{Hol}(G)$.

Aut(G), Inn(G), Out(G).

Let G be a group. As we know, the group of all automorphisms of G , denoted $\text{Aut}(G)$, is the set of all isomorphisms of a group G to itself with composition of maps as the operation. We also know that for every element $g \in G$, the map $f(g) = f_g : G \rightarrow G$ defined as $x \mapsto gxg^{-1}$ is an automorphism of G . The automorphism f_g is called the **inner automorphisms of G defined by g** , and is clear that the set $\{f_g : g \in G\}$ forms a subgroup in $\text{Aut}(G)$, denoted by $\text{Inn}(G)$. The map $g \mapsto f_g$ is a homomorphism of G to $\text{Aut}(G)$:

$$(f(gh))(x) = f_{(gh)}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = f_g(f_h(x)) = (f(g)f(h))(x),$$

hence, $f(gh) = f_{(gh)} = f(g)f(h)$ for all $g, h \in G$. Its kernel is, clearly, the center $Z = Z(G)$ of G . By the homomorphism theorem,

$$\text{Inn}(G) \cong G/Z.$$

The closer G is to an abelian group, equivalently, the larger is its center, the smaller its group $\text{Inn}(G)$ is. Only nonabelian groups have nontrivial inner automorphisms.

Let $\phi \in \text{Aut}(G)$, and $f_g \in \text{Inn}(G)$. Then, for any $x \in G$,

$$\begin{aligned} (\phi f_g \phi^{-1})(x) &= \phi(g \phi^{-1}(x) g^{-1}) = \phi(g) \phi(\phi^{-1}(x)) \phi(g^{-1}) = \phi(g) x \phi(g^{-1}) = \\ &= \phi(g) x (\phi(g))^{-1} = f_{\phi(g)}(x). \end{aligned}$$

Hence, $\phi f_g \phi^{-1} = f_{\phi(g)}$, and therefore

$$\text{Inn}(G) \trianglelefteq \text{Aut}(G).$$

Every automorphism of G which is not inner, is called **an outer automorphism of G** . As $e_{\text{Aut}(G)} = f_{e_G}$ is an inner automorphism of G , the outer automorphisms do not form a subgroup of $\text{Aut}(G)$. The group $\text{Aut}(G)/\text{Inn}(G)$ is called **the group of outer automorphisms of G** , and it is denoted by $\text{Out}(G)$:

$$\text{Out}(G) \cong \text{Aut}(G)/\text{Inn}(G).$$

Several examples are in order.

- We know that

$$\text{Aut}(\mathbb{Z}_n) \cong \text{Out}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*.$$

- It is known that for $n \geq 3$, $Z(S_n)$ is trivial. So

$$\text{Inn}(S_n) \cong S_n.$$

It can be shown, though it is not easy, that

$$\text{Aut}(S_n) \cong \text{Inn}(S_n) \cong S_n \text{ for all } n \geq 3 \text{ and } n \neq 6.$$

It can also be shown that

$$|\text{Out}(S_6)| = |\text{Aut}(S_6) : \text{Inn}(S_6)| = 2.$$

- It is known that $Z(GL(n, \mathbb{F})) = \Lambda(n, \mathbb{F}) = \{\lambda I_n : \lambda \in \mathbb{F}^*\}$. Therefore,

$$\text{Inn}(GL(n, \mathbb{F})) \cong GL(n, \mathbb{F})/\Lambda(n, \mathbb{F}).$$

The last group is often called the **projective group** and is denoted by $PGL(n, \mathbb{F})$.

Lecture 19a.**On groups of order p^3 , p is an odd prime**

The presentation below is based on Dummit and Foote [4], Hall [5], and Conrad [3]. The motivation was to make it as close as possible to the course, to use as few facts as possible, and to prove existence of exactly two isomorphism classes in nonabelian case. The latter is achieved by obtaining the description of the groups in terms of semidirect products.

Let G be a group of order p^3 , p is an odd prime. If G is abelian, using the Fundamental Theorem for Finite Abelian Groups, we get three isomorphism classes:

$$\mathbb{Z}/(p^3), \quad \mathbb{Z}/(p^2) \times \mathbb{Z}/(p) \quad \text{and} \quad \mathbb{Z}/(p) \times \mathbb{Z}/(p) \times \mathbb{Z}/(p).$$

Suppose G is not abelian. Then G contains no element of order p^3 . We use the fact that every maximal subgroup of a finite p -group is normal, which implies that every subgroup of order p^2 is normal in G . (See Corollary 7 from Lecture 9, or Theorem 22 (ii) from the Lecture Notes). Therefore our analysis can be reduced to the following two cases.

Case 1. G has an element a of order p^2 .

Let $N = \langle a \rangle$. Being of order p^2 , N is normal. As G/N is of order p , and so cyclic, there must be an element $b \in G \setminus N$ such that $b^p \in N$.

Case 1.1. $|b| = p$. Let $B = \langle b \rangle$. As $G = NB$, and $N \cap B = \langle e \rangle$,

$$G = N \rtimes_f B \quad \text{for some homomorphism} \quad f : B \rightarrow \text{Aut } N$$

Every automorphism ϕ of N is of the form $\phi_i : a \mapsto a^i$, where $(i, p^2) = 1$. Hence, there are $p^2 - p = p(p - 1)$ such automorphisms. If $f(b) = \phi_1$, then ϕ_1 is trivial, and so G is abelian as a direct product of abelian groups. Let $i = mp + r$, where $1 \leq r < p$, and $f(b) = \phi_i$. Then $|\phi_i| = |b| = p$, and therefore $a = \phi_i^p(a) = a^{i^p}$. Hence, $i^p \equiv 1 \pmod{p^2}$. As $i^p = (mp + r)^p \equiv r^p \equiv r \pmod{p}$, the latter by Fermat's theorem, and $i^p \equiv 1 \pmod{p}$, we obtain $r \equiv 1 \pmod{p}$, and so $r = 1$. Hence $f(b) = \phi_{mp+1}$, for some m , $1 \leq m < p$. For $m = 1$, we obtain $f(b) = \phi_{p+1}$. This gives us the first example of the operation in G :

$$(a^i, b^j)(a^{i'}, b^{j'}) = (a^{i+i'(p+1)}, b^{j+j'}),$$

or, identifying the set of elements of G with $\mathbb{Z}/(p^2) \times \mathbb{Z}/(p)$,

$$(i, j)(i', j') = (i + i'(p + 1), j + j').$$

Note that all $\phi_{mp+1} = \phi_{p+1}^m$ form a cyclic group of order p . We leave it for the reader to check that that the semidirect product corresponding to $f(b) = \phi_{mp+1}$ for $1 < m < p$, leads to an isomorphic group. One can do it in a way similar to the one in our solution of Problem 3 of Lecture 14 (classification of nonabelian groups of order pq , where p and q are primes and $p < q$.)

Case 1.2. $|b| = p^2$. Our goal is to show that there exists $b_1 \in G \setminus N$ of order p , and this will reduce the problem to Case 1.1.

As $G = N + bN + \dots + b^{p-1}N$, every element of $G \setminus N$ can be written in the form $b^y a^x$ for some $1 \leq x \leq p - 1$ and $1 \leq y \leq p^2 - 1$. Hence, it is sufficient to show that

for some such x and y , $|b^y a^x| = p$ and $b^y a^x$ is not in N . The latter is equivalent to b^y not in N . As $N \triangleleft G$, and b is not in N , $bab^{-1} = a^i$ for some i , where $(i, p^2) = 1$. Hence $b^j ab^{-j} = a^{i^j}$ for every j , and $b^y a^x b^{-y} = a^{xi^y}$, or $b^y a^x = a^{xi^y} b^y$. Taking $j = p$, we conclude, as we did in Case 1.1, then $i = mp + 1$ for some $1 \leq m \leq p - 1$. We have:

$$\begin{aligned} (b^y a^x)^p &= (b^y a^x) \cdot (b^y a^x) \cdot \dots \cdot (b^y a^x) = a^{xi^y} b^y \cdot (b^y a^x) \cdot \dots \cdot (b^y a^x) = \\ &= a^{xi^y} (b^{2y} a^x) (b^y a^x) \cdot \dots \cdot (b^y a^x) = a^{xi^y + xi^{2y}} b^{2y} (b^y a^x) \cdot \dots \cdot (b^y a^x) = \dots = \\ &= a^{xi^y + xi^{2y} + \dots + xi^{(p-1)y}} b^{py} = a^{x \frac{i^{py} - i^y}{i^y - 1}} b^{py} \end{aligned}$$

We wish to have

$$a^{x \frac{i^{py} - i^y}{i^y - 1}} b^{py} = 1.$$

For $y = 1$, and using $i = mp + 1$, the last equality gives

$$a^{x \frac{(mp+1)^p - (mp+1)}{mp}} b^p = a^{x(kp^2+p)} b^p = a^{xp} b^p = 1.$$

As $|b| = |a| = p^2$, and $b^p \in N$, we have $b^p = a^{pu}$ for some $u = 1, \dots, p-1$. Therefore taking $x = -u$, and setting $b_1 = a^{-u} b$, we obtain the element we were looking for!⁷

Case 2. Every nonidentity element of G has order p .

A normal subgroup H of G of order p^2 exists. We know that H must be abelian. As G contains no element of order p^2 , $H \simeq \mathbb{Z}/(p) \times \mathbb{Z}/(p)$. Let $K = \langle k \rangle$, where $k \in G \setminus H$. Then $|K| = p$, $G = HK$, and $H \cap K = \langle k \rangle$. Therefore

$$G = H \rtimes_g K \quad \text{for some homomorphism } g : K \rightarrow \text{Aut } H.$$

We know that $\text{Aut } H \simeq GL_2(\mathbb{Z}/(p))$. If $g(k)$ is the identity automorphism, then G is abelian. Hence, $|g(k)| = p$. We know that $|GL_2(\mathbb{Z}/(p))| = (p^2 - 1)(p^2 - p) = p(p-1)^2(p+1)$. Hence $g(k)$ generates a Sylow p -subgroup of $GL_2(\mathbb{Z}/(p))$. Choosing a particular Sylow p -subgroup

$$\langle g(k) = A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle < GL_2(\mathbb{Z}/(p)),$$

we obtain an operation in G :

$$(v, k^j)(v', k^{j'}) = (v + v'^{g(k)}, k^{j+j'}) = (v + v' A, k^{j+j'}).$$

Identifying the set of elements of G with $(\mathbb{Z}/(p) \times \mathbb{Z}/(p)) \times \mathbb{Z}/(p)$, we obtain

$$\begin{aligned} ((a, b), j)((a', b'), j') &= ((a, b) + (a', b')^{g(k)}, j + j') = \\ ((a, b) + (a', b') A, j + j') &= ((a, b) + (a', a' + b'), k^{j+j'}) = \\ &= ((a + a', b + a' + b'), j + j'). \end{aligned}$$

As all Sylow p -subgroups of $GL_2(\mathbb{Z}/(p))$ are conjugate, they are generated by matrices similar to A . Let $g' : K \rightarrow \text{Aut } H$ be defined by $k \mapsto CAC^{-1}$ for some $C \in GL_2(\mathbb{Z}/(p))$. Then

$$\phi : H \rtimes_g K \rightarrow H \rtimes_{g'} K, \quad (v, j) \mapsto (vC^{-1}, j),$$

is a group isomorphism, which is easily verified. Hence, all nonabelian semidirect products of H and K are isomorphic.

⁷Just trying this form of b_1 from the beginning would do, but it would not be clear how one could find it in a natural way.

Therefore there are two isomorphism classes of non-abelian groups of order p^3 , for odd prime p . \square

Though the existence of exactly two isomorphism classes in the nonabelian case is proven, it is always nice to find their examples among familiar groups. One can show that our first construction is isomorphic to the group

$$G_p = \left\{ \begin{pmatrix} 1 + (p) & b \\ 0 & 1 \end{pmatrix}, (p) = p\mathbb{Z}/(p^2), \text{ and } b \in \mathbb{Z}/(p^2) \right\},$$

and our second construction is isomorphic to the $UT_3(\mathbb{Z}/(p))$, also known as Heisenberg group:

$$UT_3(\mathbb{Z}/(p)) = \text{Heis}(\mathbb{Z}/(p)) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, a, b, c \in \mathbb{Z}/(p). \right\}$$

We leave it to the reader to find subgroups of G_p isomorphic to N and B , subgroups of $\text{Heis}(\mathbb{Z}/(p))$ isomorphic to H and K , and establish related isomorphisms. In case of difficulties, one can consult [3].

Lecture 20.

Wreath product of permutation groups.

Wreath product of permutation groups, which we are going to discuss in this lecture, is a very natural notion. It can be used to describe the Sylow's subgroups of the symmetric group S_n , the automorphism group of the binary n -cube Q^n , and automorphism groups of other graphs.

Instead of starting with a definition of the wreath product, we consider the following problem. Take five sets $B_i = \{x_i, y_i\}$, $i \in [5]$, we call them blocks whose union $\bigcup_{i \in [5]} B_i$ contains 10 elements. Let G be a group of all permutations of these 10 elements, which induces a permutation on the set of blocks.

Every such a permutation can be thought of being performed in two steps: first we permute elements inside some blocks, then we permute blocks. Let us represent x_i and y_i as (x, i) and (y, i) respectively, i.e., as elements of $U = \{x, y\} \times [5]$. Let

$$F = \{f : [5] \rightarrow \text{Sym}(\{x, y\})\}$$

denote the set of all functions from $[5]$ to $\text{Sym}(\{x, y\})$. Then any element of G can be represented as $[f, \pi]$, where $f \in F$, and $\pi \in \text{Sym}([5]) = S_5$.

Let us define a map

$$[f, \pi] : U \rightarrow U \quad \text{such that} \quad (z, i) \mapsto ((f(i))(z), \pi(i)) = (z^{f(i)}, i^\pi).$$

Since the product in G is the composition of permutations, we have that the product of $[f, \pi]$ and $[h, \sigma]$ should map (z, i) to

$$\begin{aligned} (z, i)^{[f, \pi][h, \sigma]} &= ((z, i)^{[f, \pi]})^{[h, \sigma]} = (z^{f(i)}, i^\pi)^{[h, \sigma]} = \\ &= ((z^{f(i)})^{h(i^\pi)}, (i^\pi)^\sigma) = (z^{f(i)h(i^\pi)}, i^{\pi\sigma}) \end{aligned}$$

Note that $f(i)h(i^\pi)$ in $z^{f(i)h(i^\pi)}$ is a product of two elements of $\text{Sym}(\{x, y\})$.

In order to reduce the operation to a more familiar one, we wish to rewrite the function $i \mapsto h(i^\pi)$ in a different way. Consider a function $h^\pi \in F$ defined by $i \mapsto h(i^\pi)$. Then $f(i)h(i^\pi) = f(i)h^\pi(i) = (fh^\pi)(i)$, where fh^π is understood as a usual pointwise product of functions in F . Note also that with respect to *this* multiplication, F is a group. Thus, the operation in G can be presented as

$$[f, \pi][h, \sigma] = [fh^\pi, \pi\sigma],$$

which looks very similar to the definition of an external semidirect product of groups F and S_5 . In order to be convinced that it really is, we first

(1) describe the homomorphism $g : S_5 \rightarrow \text{Aut}(F)$ needed in the definition of a semidirect product of F and S_5 , and then

(2) check that $F \cong F \times \{e\} \trianglelefteq G$, where e is the identity element of S_5 , and $S_5 \cong \{1_G\} \times S_5 \leq G$.

Note also that in our notations, the identity element of G is $[1_F, e_{S_5}]$, where $e = e_{S_5}$ is the identity element in S_5 , and 1_G is the identity function in F : $1_G(i) = e$ for all $i \in [5]$. The inverse $[f, \pi]^{-1}$ of $[f, \pi]$ is $[(f^{-1})^{\pi^{-1}}, \pi^{-1}]$.

Let's check (1). For any $\alpha \in S_5$, consider a map g_α on F defined by $f \mapsto f^\alpha$ as above: $f^\alpha(i) = f(i^\alpha)$ for all $i \in [5]$. Clearly, $f^\alpha \in F$. We have to check that g_α is an automorphism of F and that $g_{\alpha\beta} = g_\alpha g_\beta$. Let us do it.

Why is g_α a bijection? If $g_\alpha(f_1) = g_\alpha(f_2)$, then $f_1^\alpha(i) = f_2^\alpha(i)$ for all i , which is equivalent to $f_1(i^\alpha) = f_2(i^\alpha)$ for all i . As α is a bijection on $[5]$, this gives $f_1 = f_2$. Therefore g_α is injective. As F is finite, g_α is bijective.

Why is g_α a homomorphism?

$$(g_\alpha(f_1 f_2))(i) = (f_1 f_2)^\alpha(i) = (f_1 f_2)(i^\alpha) = f_1(i^\alpha) f_2(i^\alpha) = f_1^\alpha(i) f_2^\alpha(i) = (g_\alpha(f_1))(i) (g_\alpha(f_2))(i) = (g_\alpha(f_1))(g_\alpha(f_2))(i),$$

hence $g_\alpha(f_1 f_2) = g_\alpha(f_1) g_\alpha(f_2)$ and g_α is a homomorphism. Since g_α is bijective, it is an automorphism of F .

Let's check (2). Why is $F \times \{e\} \trianglelefteq G$? For any $f \in F$, and $[g, \alpha] \in G$,

$$[g, \alpha][f, e][g, \alpha]^{-1} = [h, \alpha][k, \alpha^{-1}] = [gh^\alpha, e],$$

where $h, k \in \mathbb{F}$. Hence, $F \cong F \times \{e\} \trianglelefteq G$. The proof that $\{1_G\} \times S_5 \leq G$ is trivial.

Therefore we proved that

$$G = F \rtimes_g S_5,$$

where $g : S_5 \rightarrow \text{Aut}(F)$ defined via $\alpha \mapsto g_\alpha$, with $g_\alpha(f) = f^\alpha$. Group G acts on the set $x, y \times [5]$ by the rule: $(z, i)^{[f, \pi]} = (z^{f(i)}, i^\pi)$. We denote group G by $S_2 \wr S_5$ and call it the **wreath product of S_2 and S_5** . We have $|G| = 2^5 \cdot 5!$.

Let us generalize the construction in the example above. All verifications are similar, and we will not repeat them. Consider two permutation groups: A on a

set X and B on a set Y . Let $F = A^Y$ denote the set of all functions from the set Y to group A . F is a group with respect to pointwise multiplication of functions. For $b \in B$ and any $f \in F$, let $f^b \in F$ be a function defined as $f^b(y) = f(y^b)$ for all $y \in Y$. Then the map $\phi : f \mapsto f^b$ is an automorphism of F , and the group

$$G = F \rtimes_\phi B,$$

is called the **wreath product of permutation groups (A, X) and (B, Y)** , and is denoted by $A \wr B$. The product of elements of G is defined as

$$[f_1, b_1][f_2, b_2] = [f_1 f_2^{b_2}, b_1 b_2].$$

We have $|G| = |A|^{|Y|} \cdot |B|$. G can be considered as a permutation group on $X \times Y$, where

$$(x, y)^{[f, b]} = (x^{f(y)}, y^b).$$

Wreath product of abstract groups.

Let A and B be groups, and let $F = A^B$ denote the set of all functions from B to A . F is a group with respect to pointwise multiplication of functions. For $b \in B$

and any $f \in F$, let $f^b \in F$ be a function defined as $f^b(y) = f(by)$ for all $y \in B$. Then the map $\phi : f \mapsto f^b$ is an automorphism of F , and the group

$$G = F \rtimes_{\phi} B,$$

is called the **wreath product of groups A and B** , and is denoted by $A \wr B$. The product of elements of G is defined as

$$[f_1, b_1][f_2, b_2] = [f_1 f_2^{b_2}, b_1 b_2].$$

We have $|G| = |A|^{|B|} \cdot |B|$.

Examples.

- the original example generalized to $S_k \wr S_n$.
- regular tree with all non-leaves of degree 3 and depth 2: $\text{Aut}(\Gamma) \simeq S_2 \wr S_3$.
- $\text{Aut}(K_3 + K_3) \simeq S_3 \wr S_2$.
 $K_3 + K_3$ denotes the graph which is union of two disjoint triangles.
- $\text{Aut}(\vec{C}_4 + \vec{C}_4) \simeq \mathbb{Z}_4 \wr S_2$.
 $\vec{C}_4 + \vec{C}_4$ denotes the graph which is union of two disjoint directed cycles on four vertices.
- $\text{Aut}(T_3(6)) \simeq S_2 \wr S_3 \simeq \text{Aut}(3K_2)$.
 $T_3(6)$ denotes the complete 3-partite graph on 6 vertices, and $3K_2$ denotes the complement of $T_3(6)$, which is the union of three disjoint edges.

An important property of the wreath product is that it is associative:

$$(A \wr B) \wr C \simeq A \wr (B \wr C).$$

The verification is left to the reader. For permutation groups, the corresponding permutation groups are similar.

Lecture 21.

Sylow subgroups of S_n .

The goal of this section is to describe the structure of p -Sylow's subgroups of the symmetric group S_n in terms of the direct product of permutation groups and wreath product of permutation groups. It was suggested by L.A. Kalužnin in 1948.

We remind the reader that the direct product of n permutation groups (G_i, X_i) is a the permutation group (G, X) , where $X = X_1 \times \dots \times X_n$, $G = G_1 \times \dots \times G_n$, and $g = (g_1, \dots, g_n) \in G$ acts on $x = (x_1, \dots, x_n)$ as $x \mapsto x^g = (x_1^{g_1}, \dots, x_n^{g_n})$.

Let $\exp_p(N)$ denote the greatest integer a such that p^a divides N . Then it is easy to see that

$$\exp_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots + \left\lfloor \frac{n}{p^k} \right\rfloor + \dots \quad (0.6)$$

Hence the order of a p -Sylow subgroup G of S_n is $|G| = p^{\exp_p(n!)}$, and for $n = p^m$,

$$|G| = p^{p^{m-1} + p^{m-2} + \dots + p + 1}. \quad (0.7)$$

As all p -Sylow subgroups are conjugate, they are isomorphic, and, hence, it is sufficient to study one of them.

In order to do this, we write n in base p :

$$n = a_u p^u + a_{u-1} p^{u-1} + \dots + a_1 p + a_0, \quad 0 \leq a < p. \quad (0.8)$$

Then

$$\begin{aligned} \exp_p(n!) &= (a_u p^{u-1} + \dots + a_1) + (a_u p^{u-2} + \dots + a_2) + \dots = \\ &= a_u (p^{u-1} + \dots + p + 1) + a_{u-1} (p^{u-2} + \dots + p + 1) + \dots + a_1. \end{aligned}$$

Hence

$$\begin{aligned} |G| &= p^{a_u (p^{u-1} + \dots + p + 1) + a_{u-1} (p^{u-2} + \dots + p + 1) + \dots + a_1} = \\ &= (p^{p^{u-1} + \dots + p + 1})^{a_u} \cdot (p^{p^{u-2} + \dots + p + 1})^{a_{u-1}} \cdot \dots \cdot (p^{p+1})^{a_2} \cdot p^{a_1}. \end{aligned} \quad (0.9)$$

Partition $[n]$ into a_u blocks of p^u elements in each block, a_{u-1} blocks of p^{u-1} elements in each block, and so on, a_1 blocks of p elements in each block, and a_0 blocks of 1 element in each block. Hence $[n]$ is partitioned into $a_u + \dots + a_0$ blocks. For each block B , consider a p -Sylow subgroup $Syl(B)$ of the symmetric group $Sym(B)$. Then take the direct product of all permutation groups $(Syl(B), B)$. Computing the order of the direct product, we obtain that it is given by (0.9). The degree of the direct product (i.e., the number of points of the permutation group) is n (by (0.8)). As all p -Sylow subgroups of S_n are conjugate, the direct product is isomorphic to G considered as a permutation group on $[n]$.

Therefore, what is left is to describe the structure of the factors of this direct product, i.e., of $(Syl(B), B)$.

Suppose $|B| = p^m$, $m = 1, \dots, u$. The order of $Syl(B)$ is given by (0.7). We observe that for $m = 1, 2, 3$, it is p , p^{p+1} , p^{p^2+p+1} , respectively. These numbers coincide with the orders of \mathbb{Z}_p , $\mathbb{Z}_p \wr \mathbb{Z}_p$, $\mathbb{Z}_p \wr \mathbb{Z}_p \wr \mathbb{Z}_p$, respectively. This suggests the following recursive construction.

Let A_m be a p -Sylow subgroup of S_{p^m} of degree p^m and $B = (\mathbb{Z}_p, [p])$. Then

$$|A_m \wr B| = |A_m|^p \cdot |B| = (p^{p^{m-1} + \dots + p + 1})^p \cdot p = p^{p^m + \dots + p + 1} = \exp_p(p^{m+1}).$$

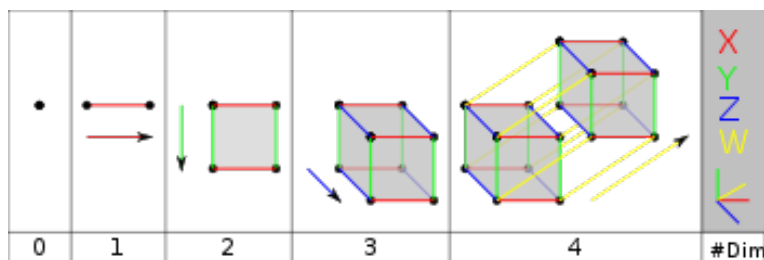
As the wreath product of A_m and B acts on the direct product of $[p^m]$ and $[p]$, its degree is p^{m+1} . Therefore it is isomorphic to A_{m+1} acting on $[p^{m+1}]$.

We have proved the following theorem.

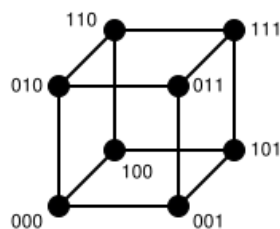
Theorem 33. (L.A. Kalužnin, 1948.) *Let $n = a_u p^u + a_{u-1} p^{u-1} + \dots + a_1 p + a_0$, $0 \leq a < p$. Then each p -Sylow subgroup of S_n is isomorphic to the direct product of a_i groups $\mathbb{Z}_p \wr \dots \wr \mathbb{Z}_p$ (i copies), over all $i = 0, \dots, u$.*

Automorphism group of binary n -cube.

There are several ways to define the graph Q_n , which is often called the a binary n -cube.⁸



$Q_n, n = 0, \dots, 4.$



Q_3 as \mathbb{Z}_2^3

1. The vertex set $V(Q_n)$ is \mathbb{Z}_2^n viewed as the n -dimensional vector space over \mathbb{Z}_2 . Two vertices (vectors) u, v form an edge of Q_n if and only if they differ in exactly one component. Obviously, $|V(Q_n)| = 2^n$, every vertex of Q_n has degree n , and $|E(Q_n)| = n2^{n-1}$. It is obvious that the elementary abelian group \mathbb{Z}_2^n acts on itself via

$$\hat{g} : x \mapsto x + g,$$

and $uv \in E(Q_n)$ if and only if $\hat{g}(u)\hat{g}(v) \in E(Q_n)$. Therefore \hat{g} is an automorphism of Q_n . This action is obviously transitive and faithful.

The symmetric group S_n acts on $V(Q_n)$ by simultaneously permuting component of vectors: for any $\pi \in S_n$, define

$$\hat{\pi} : (u_1, \dots, u_n) \mapsto (u_{1\pi}, \dots, u_{n\pi}).$$

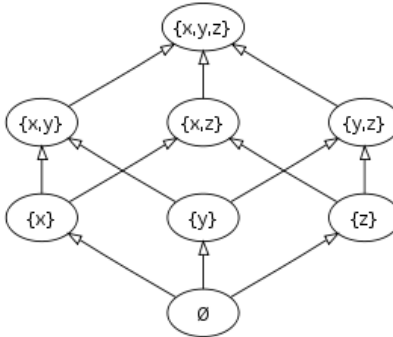
⁸The images licensed by Creative Commons (CC).

It is obvious again that $uv \in E(Q_n)$ if and only if $\hat{\pi}(u)\hat{\pi}(v) \in E(Q_n)$. Therefore $\hat{\pi}$ is an automorphism of Q_n . This action is obviously faithful.

Hence, we have two subgroups of $\text{Aut}(Q_n)$: one isomorphic to group \mathbb{Z}_2^n , and another to S_n . Let's denote them by $\widehat{\mathbb{Z}}_2^n$ and \widehat{S}_n . It is also clear that the only automorphism of Q_n these subgroups share is the identity one. (Why?) It is also easy to check that for any $\hat{\pi}$, $\hat{\pi}^{-1}\widehat{\mathbb{Z}}_2^n\hat{\pi} = \widehat{\mathbb{Z}}_2^n$. This implies that $\widehat{\mathbb{Z}}_2^n \times \widehat{S}_n \leq \text{Aut}(Q_n)$, and that $|\widehat{\mathbb{Z}}_2^n \times \widehat{S}_n| = 2^n n!$.

2. Another way to view the set of vertices of Q_n is as the set $F = \mathbb{Z}_2^{[n]}$ of all functions $f : [n] \mapsto \mathbb{Z}_2$. It is clear that there is a bijection between the set F and the vector space \mathbb{Z}_2^n : $f \mapsto (f(1), \dots, f(n))$. The adjacency relation is defined as: a pair of functions forms an edge if and only if they differ on exactly one element of $[n]$. It is clear that this graph is isomorphic to Q_n described above. F is an abelian group with respect to pointwise addition of function. It is clear that an action of F on itself via $\hat{g} : f \mapsto f + g$, or of S_n on F via $\hat{\pi} : f \mapsto f^\pi$, where $f^\pi(i) = f(i^\pi)$, result in automorphisms of the graph Q_n . As before, one can see that \widehat{S}_n normalizes F in $\text{Aut}(Q_n)$, that $\widehat{F} \times \widehat{S}_n \leq \text{Aut}(Q_n)$, and that $|\widehat{F} \times \widehat{S}_n| = 2^n n!$. Identifying \mathbb{Z}_2 with S_2 , we can also present $\widehat{F} \times \widehat{S}_n$ as $S_2 \wr S_n$. Note that usual action of $S_2 \wr S_n$ is on the set of $2n$ points, as in our case the same abstract group acts on 2^n points.

3. Our third way of viewing graph Q_n is the following. For each vector $u = (u_1, \dots, u_n) \in \mathbb{Z}_2^n$, let $U = \{i \in [n] : u_i = 1\}$. Then $V(Q_n)$ can be viewed as $2^{[n]}$ – the set of all subset of $[n]$. Two subsets U and V form an edge if and only if their symmetric difference $U \Delta V = (U \setminus V) \cup (V \setminus U)$ contains exactly one element. The elements of the standard basis in \mathbb{Z}_2^n correspond to the 1-element subsets of $[n]$, and the vectors with exactly i coordinates equal 1 correspond to i -element subsets. If we identify \mathbb{Z}_2^n with $2^{[n]}$, then $2^{[n]}$, being a group with respect to symmetric difference operation, acts on itself by symmetric difference. The action of S_n on $2^{[n]}$ is the induced action of its natural action on $[n]$. Note that with this interpretation of $V(Q_n)$, every set of k elements, $0 \leq k \leq n$ is at distance k from \emptyset , and its adjacent to all k of its $(k-1)$ -element subsets and to all $n-k$ of its $(k+1)$ supersets in $[n]$.



Q_3 as (undirected) Hasse diagram of the poset $2^{[3]}$.⁹

⁹The image licensed by Creative Commons (CC).

Now we will explain that $G = \widehat{\mathbb{Z}}_2^n \rtimes \widehat{S}_n$ (or $\widehat{F} \rtimes \widehat{S}_n$) is actually the whole automorphism group of Q_n . In what follows we use our third model of Q_n , and we show that the stabilizer of the vertex \emptyset of Q_n in $A = \text{Aut}(Q_n)$ is isomorphic to S_n . As G is transitive on $V(Q_n)$, so is A . This implies $|A| = 2^n n!$, and we get $G = A$. Here is the argument.¹⁰

We can partition vertices of Q_n according to their distance in the graph to vertex \emptyset . Let M_i represent the set of all vertices at distance i from \emptyset in Q_n , $i = 0, 1, \dots, n$. It is clear that $\widehat{S}_n \leq A_\emptyset$ and both groups acts on each M_i . (Why?) Let us show that $A_\emptyset \leq \widehat{S}_n$.

Suppose $a \in A_\emptyset$. The automorphism a acts on M_1 as a permutation. Elements of M_1 are all 1-element subsets of $[n]$. Let $g \in S_n$ be such that $\{i\}^a = \{i^g\} = \{i\}^{\hat{g}}$. Now $a\hat{g}^{-1}$ fixes all the vertices of $M_0 \cup M_1$. We want to show that it fixes all vertices of Q_n . Proceeding by induction, we suppose it fixes all elements of $M_0 \cup M_1 \cup \dots \cup M_i$ for all i , $0 \leq i < k$. If $U \in M_k$ with $k \geq 2$, then there are exactly k sets $U_1, \dots, U_k \in M_{k-1}$ adjacent to U in Q_n , and $U (= U_1 \cup \dots \cup U_k)$ is the only set in M_k adjacent to each U_i . By induction hypothesis, the vertices U_1, \dots, U_k are fixed by $a\hat{g}^{-1}$, and hence (by its uniqueness) so is U . Therefore $a\hat{g}^{-1}$ fixes each vertex of M_k , and therefore all vertices of Q_n . Therefore, $a\hat{g}^{-1}$ is the identity element of A , and so $a = \hat{g}$. This proves that $A_\emptyset \leq \widehat{S}_n$. Hence, $A_\emptyset = \widehat{S}_n$, and

$$\text{Aut}(Q_n) \cong \widehat{\mathbb{Z}}_2^n \rtimes S_n \cong S_2 \wr S_n.$$

¹⁰The proof is a slight modification of the argument in G. Jones, M.H. Klin, F. Lazebnik [8].

Lectures 22 – 23.Isometries of \mathbb{R}^n

For $x = (x_1, \dots, x_n) \in \mathbb{R}^n$, let $\|x\| = (\sum_{i=1}^n x_i^2)^{1/2}$ denote the euclidian norm of $x \in \mathbb{R}^n$ or the **length** of x , and $\|x - y\|$ denote the corresponding euclidian **distance** between x and y . Consider a function $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ such that for every $x, y \in \mathbb{R}^n$, $\|f(x) - f(y)\| = \|x - y\|$. Such a function is called an **isometry** on \mathbb{R}^n . In other words, isometries are the maps on \mathbb{R}^n which preserve distances between points. Sometimes isometries are called **congruences**. As $\|x\| = 0$ if and only if $x = 0$, any isometry is an injection. Is every isometry a surjection? (???) We will answer this question later in this section.

The reader may know that in \mathbb{R}^2 and \mathbb{R}^3 any isometry is a composition of a translation and an orthogonal transformation. Our goal is to prove the following more general result.

Theorem 34. *A function $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ is an isometry if and only if for every $x \in \mathbb{R}^n$, $f(x) = g(x) + a$, where g is an orthogonal transformation of \mathbb{R}^n and a is a (constant) vector. Equivalently, every isometry is a composition of an orthogonal transformation and a translation, and such a representation is unique.*

Proof. Consider $g(x) = f(x) - f(0)$. Then for every $x, y \in \mathbb{R}^n$,

$$\|g(x) - g(y)\| = \|f(x) - f(y)\| = \|x - y\|.$$

Hence, g is a distance preserving map. As $g(0) = f(0) - f(0) = 0$, for every $x \in \mathbb{R}^n$,

$$\|g(x)\| = \|g(x) - 0\| = \|g(x) - g(0)\| = \|x - 0\| = \|x\|.$$

Hence, g preserves the lengths of vectors. Let $x \cdot y = \sum_{i=1}^n x_i y_i$ denote the standard dot product on \mathbb{R}^n . Then $x \cdot x = \|x\|^2$.

Lemma 3. *If g is a map on \mathbb{R}^n which preserves length of all vectors, then g is a linear map.*

Proof. First we observe that $\|x - y\|^2 = (x - y) \cdot (x - y) = \|x\|^2 - 2x \cdot y + \|y\|^2$. Therefore,

$$x \cdot y = \frac{1}{2} (\|x\|^2 + \|y\|^2 - \|x - y\|^2) = \frac{1}{2} (\|g(x)\|^2 + \|g(y)\|^2 - \|g(x - y)\|^2) = g(x) \cdot g(y).$$

Hence, g preserves the dot product of vectors. We show that this implies that g is a linear map via the following argument. First we note that g maps every orthonormal basis $\{e_1, \dots, e_n\}$ of \mathbb{R}^n to a set $\{g(e_1), \dots, g(e_n)\}$ of unit vectors which are mutually orthogonal. Hence, they also form an orthonormal basis of \mathbb{R}^n (why?). Secondly, if $x = \sum_{i=1}^n x_i e_i$, and $g(x) = \sum_{i=1}^n y_i g(e_i)$ then

$$x_i = x \cdot e_i = g(x) \cdot g(e_i) = y_i$$

for all i . Therefore,

$$g(x) = g\left(\sum_{i=1}^n x_i e_i\right) = \sum_{i=1}^n x_i g(e_i),$$

which immediately implies that

$$g(x + y) = g(x) + g(y) \quad \text{and} \quad g(\lambda x) = \lambda g(x)$$

for all $x, y \in \mathbb{R}^n$ and all $\lambda \in \mathbb{R}$. Hence, g is linear map on \mathbb{R}^n . \square

As $g = f - f(0)$, g is injective. Being linear and injective, g is surjective, and, hence, so is f . Thus we have established the surjective property of f mentioned at the beginning of the lecture. Moreover, we have established that g is an orthogonal map on \mathbb{R}^n , as it is linear and preserves the length of all vectors (or, equivalently, carries every orthonormal basis to an orthonormal basis). Let $a \in \mathbb{R}^n$, and T_a be a map on \mathbb{R}^n defined by $x \mapsto x + a$. T_a is called a translation of \mathbb{R}^n by a . Clearly, T_a is an isometry, and $T_a^{-1} = T_{-a}$. Hence, we have $f = T_a \circ g$. If the same f can be written as $f = T_{a'} \circ g'$, then $T_a \circ g = T_{a'} \circ g'$, which is equivalent to $T_{-a'+a} = g' \circ g^{-1}$. Since both g' and g^{-1} map 0 to 0, and $T_{-a'+a}$ maps 0 to $-a' + a$, we get $-a' + a = 0$. Hence, $a = a'$, $T_a = T_{a'}$, and so $g = g'$. This proves that the representation $f = T_a \circ g$ is unique, and finishes the proof of the theorem. \square

As an inverse of an isometry is an isometry, all isometries of \mathbb{R}^n form a group under the composition, the **group of isometries** of \mathbb{R}^n which is denoted by $Iso = Iso(n, \mathbb{R})$. It is easy to see (check!) that $(T_a \circ g)^{-1} = T_{-g^{-1}(a)} \circ g^{-1}$. Let $O = O(n, \mathbb{R})$ denote the orthogonal group of \mathbb{R}^n (or the corresponding group of orthogonal matrices), and T denote the group of all translations of \mathbb{R}^n . Clearly, T is isomorphic to the additive group of \mathbb{R}^n . It is easy to check (do it!) that $O \triangleleft Iso$. As $Iso = OT$, we obtain that $Iso \cong O \rtimes T$.

Using matrices, every isometry can be written as

$$x \mapsto Ax + a,$$

where $A \in O$ (the set of orthogonal matrices), and a, x are column vectors.

Thought as a matrix, every element of O has determinant 1 or -1 . Indeed, for every orthogonal matrix A , $AA^t = I$, which gives $(\det A)^2 = 1$, or $|\det A| = 1$. If $\det A = 1$, A , or the corresponding orthogonal transformation, is called a **rotation**, or **rigid motion**. If $\det A = -1$, A , or the corresponding orthogonal transformation, is called a **reflection**, or **rigid motion**. The map $A \mapsto \det A$ defines a surjective homomorphism of O to $\{1, -1\}$. Its kernel is denoted by $O^+ = O^+(n, \mathbb{R})$ consists of all rotations, and it is often referred to as the group of rotations. Clearly, $O^+ \triangleleft O$ and $|O : O^+| = 2$.

The terms 'rigid motion' or 'rotation' reflect the fact that in \mathbb{R}^n , $n = 2, 3$, they correspond to actual mechanical motions which fix a point. They also are the **orientation preserving** transformations, the notion we do not define here.

Finite groups of isometries of \mathbb{R}^n

If a group of isometries contains a translation by a nonzero vector, the group must be infinite. Therefore, if we wish to study finite subgroups of isometries, they must form a subgroup in O . These finite groups played an important role in the development of group theory, and we begin discussing them now.

We allow ourselves to use standard facts from linear algebra concerning orthogonal transformations of \mathbb{R}^n . In order to understand finite subgroups of O , we first do it for O^+ . For n odd, every matrix of O^+ has a real eigenvalue since its characteristic polynomial is of odd degree, and so it is 1. This means that A fixes a nonzero vector.

$n = 1 : O^+ = O^+(1, \mathbb{R})$.

Let v be a nonzero fixed vector of $A \in O$. As every $x \in \mathbb{R}^1$ is a multiple of v , A is the identity map, and so $O^+(1, \mathbb{R})$ is the identity group.

$n = 2 : O^+ = O^+(2, \mathbb{R})$.

Let $A \in O^+$. If A has a real eigenvalue, then all two of its eigenvalues are real, and both must be equal 1. Thus A is the identity map in this case. If A has no real eigenvalues, then it is well known that A can be represented by a rotation matrix $R(\theta)$, for some $\theta \in (0, 2\pi)$, i.e.,

$$A = R(\theta) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

Let G be a nontrivial finite subgroup of O^+ . Then $|G| = m \geq 2$. Among all nonidentity rotations forming G , we chose the one with the *least positive* angle θ . For any $R(\alpha) \in G$, we have $\alpha = q\theta + \beta$, where q is a positive integer and $0 \leq \beta < \theta$. Then $R(\beta) = R(\alpha - q\theta) = (R(\theta))^{-q} \circ R(\alpha) \in G$, and therefore $\beta = 0$. This implies that every element of G can be thought as $R(q\theta)$, for $q = 1, \dots, m$, where $m\theta = 2\pi$. Hence, G is a cyclic group of order m generated by $R(2\pi/m)$. This completely describes $O^+(2, \mathbb{R})$.

$n = 3 : O^+ = O^+(3, \mathbb{R})$.

Let G be a nontrivial finite subgroup of O^+ of order $m \geq 2$. As 3 is odd, for every $A \in O^+$, there exists a fixed nonzero eigenvector x of unit length. Then A fixes all vectors of $\langle x \rangle$, and can be thought as a rotation in \mathbb{R}^3 around $\langle x \rangle$ in the plane $\langle x \rangle^\perp$. If the order of A in G is $p \geq 1$, then the restriction of $\langle A \rangle$ on $\langle x \rangle^\perp$ is a finite subgroup of $O^+(2, \mathbb{R})$ of order p , and, as was shown above, it must be a cyclic group of order p . If $p = 1$, then A is the identity map. Let us assume that $p \geq 2$.

Obviously G acts on the unit sphere $S^2 = \{z \in \mathbb{R}^3 : \|z\| = 1\}$. As A is not the identity map, it fixes exactly two points of S^2 , namely x and $-x$, which we call the **poles** of A , and we say that the **order** of these poles is $p_x = p$. It is clear that distinct nonidentity elements of G have distinct set of poles, and so G has $N = 2(m - 1)$ poles.

It turns out that G acts on the set of its all poles!

Lemma 4. *Let G be a finite subgroup of $O^+(3, \mathbb{R})$, and x be a pole of $h \in G$, $h \neq e$. Then x^g is a pole of G for every $g \in G$.*

Proof. Let $g \in G$. As $(x^g)^{g^{-1}hg} = x^{hg} = x^g$, vector x^g is a fixed vector of $g^{-1}hg \in G$. Since $h \neq e$, then $g^{-1}hg \neq e$. Therefore x^g is a pole of $g^{-1}hg$, and so G acts on the set of all its poles. \square

Consider all orbits of G acting on the set of all its poles. An orbit containing a pole x has length $|G : G_x|$, where G_x is the stabilizer of x in G . As we know, G_x is a cyclic group of order p_x . Therefore, we count the number of elements in the set

$$S = \{(x, g) : x \text{ is a pole of } g, g \in G \setminus \{e\}\},$$

in two different ways. For a fixed $g \in G \setminus \{e\}$, there are exactly two poles of g . Hence, $|S| = N = 2(m-1)$. On the other hand, a pole x is a pole to exactly $p_x - 1$ elements of G , namely the nonidentity elements of the cyclic group $\langle g \rangle$. Hence,

$$|S| = \sum_x (p_x - 1),$$

where the summation is over all poles. Grouping all poles from an orbit of G , we rewrite the last summation as

$$|S| = \sum_x (p_x - 1) = \sum'_x (p_x - 1) \frac{m}{p_x},$$

where \sum'_x is over the set of representatives of all orbits, one for each orbit. Therefore we have

$$N = 2(m-1) = \sum'_x (p_x - 1) \frac{m}{p_x},$$

or, equivalently

$$2 - \frac{2}{m} = \sum'_x \left(1 - \frac{1}{p_x}\right), \quad (0.10)$$

where, again, the summation is taken over the set of representatives of all orbits, one for each orbit. Now we will use equation (0.10) to describe all finite subgroups of $O^+(3, \mathbb{R})$. The main observation is that the l.h.s. of (0.10) is less than 2, and for large p_x , $1 - \frac{1}{p_x}$ is close to 1. Hence, not many p_x can be large. Note also that p_x must be a divisor of m .

Here we go over all solutions of (0.10), and discuss their properties and groups behind them.

We claim that the number t of orbits of G on the set of poles is at most three. Indeed, if $t \geq 4$, we would have

$$\begin{aligned} 2 - \frac{2}{m} &= \left(1 - \frac{1}{p_x}\right) + \left(1 - \frac{1}{p_y}\right) + \left(1 - \frac{1}{p_z}\right) + \cdots + \left(1 - \frac{1}{p_w}\right) \Leftrightarrow \\ t - 2 + \frac{2}{m} &= \frac{1}{p_x} + \frac{1}{p_y} + \frac{1}{p_z} + \cdots + \frac{1}{p_w}. \end{aligned}$$

As each order of the pole is at least 2, the sum of their reciprocals is at most $t/2$. As $t - 2 + \frac{2}{m} > t/2$ for $t \geq 4$, the last equations has no solutions in positive integers. Hence, $1 \leq t \leq 3$. The results of going through these several cases are below.

- (i) $t = 1$. Then $2 - \frac{2}{m} = 1 - \frac{1}{p_x}$. As the l.h.s is at least 1 and the r.h.s. is less than 1, this equation has no solutions in positive integers.
- (ii) $t = 2$. Then $2 - \frac{2}{m} = \left(1 - \frac{1}{p_x}\right) + \left(1 - \frac{1}{p_y}\right)$, which is equivalent to $\frac{2}{m} = \frac{1}{p_x} + \frac{1}{p_y}$, or to

$$2 = \frac{m}{p_x} + \frac{m}{p_y}.$$

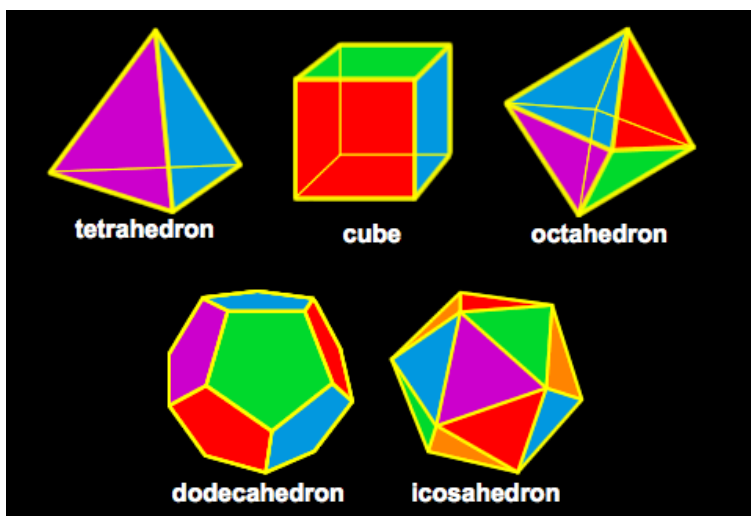
As both fractions on the right are positive integers, and they add to 2, $p_x = p_y = m$. As the length of the orbit containing x is m/p_x , each of our orbit has one pole. Thus we have two orbits of poles of order m , each containing one pole. So G is a cyclic group of order m of rotations around the line defined by the two (opposite) poles.

(iii) $t = 3$. Then (0.10) is equivalent to

$$1 + \frac{2}{m} = \frac{1}{p_x} + \frac{1}{p_y} + \frac{1}{p_z}. \quad (0.11)$$

We may assume that $2 \leq p_x \leq p_y \leq p_z$, otherwise the poles could be relabeled in order to satisfy this condition. Then $p_x = 2$, otherwise the sum of three fractions on the right is less than 1, but $1 + \frac{2}{m} > 1$.

- (a) $p_x = p_y = 2$. If $p_z = p$, then $m = 2p$. This implies that m is even and there are two orbits of poles of order 2, each orbit having p poles, and one orbit consisting of two poles of order p . The group G contains a rotation of order p around the line l defined by two poles of the third orbit, and p rotations of order 2 around p lines perpendicular to l . It is easy to argue that in this case G is isomorphic to the dihedral group D_{2p} – group of all symmetries of a (plane) regular $2p$ -gon. Note that the rotations of order two are in \mathbb{R}^3 . They correspond to reflections with respect to axes of symmetry of the regular $2p$ -gon in \mathbb{R}^2 .
- (b) $p_x = 2, 4 \leq p_y \leq p_z, p_x = 2, p_y = 3, 6 \leq p_z$: none of these provides a solution to (0.11).
- (c) $p_x = 2, p_y = p_z = 3, m = 12$. There exists one orbit of 6 poles of order 2, and two orbits of poles of order 3, each containing 4 poles. An example of such group G is the group of rotations of a regular tetrahedron. 3 pairs of 6 poles of order 2 correspond to 3 lines passing through the midpoints of skew edges of the tetrahedron. Poles of order 3 correspond to the medians of the tetrahedron (lines passing through a vertex and the centroid of opposite face). As a permutation group this group is similar to A_4 , and one can argue that there is no other isomorphic class in this case.
- (d) $p_x = 2, p_y = 3, p_z = 4, m = 24$. Here we have one orbit of 12 poles of order 2, one orbit of 8 poles of order 3, and one orbit of 6 poles of order 4. An example of such group G is the group Q of rotations of a cube (or a regular octahedron). 12 poles of order 2 correspond to the lines passing through the midpoints of opposite parallel edges (not in one face). 8 poles of order 3 correspond to four long diagonals lines of the cube. 6 poles of order 4 correspond to the lines passing through the centers of opposite faces. The group Q is isomorphic to S_4 , and one can argue that there is no other isomorphic class in this case.
- (e) $p_x = 2, p_y = 3, p_z = 5, m = 60$. Here we have one orbit of 30 poles of order 2, one orbit of 20 poles of order 3, and one orbit of 12 poles of order 5. An example of such group G is the group Y of rotations of a regular dodecahedron (or a regular icosahedron). It contains 30 poles of order 2, 20 poles of order 3, and 12 poles of order 5. The group Y is isomorphic to A_5 , and one can argue that there is no other isomorphic class in this case.



Convex Regular Polyhedra in \mathbb{R}^3 .¹¹

We collect our findings in the following theorem.

Theorem 35. *Every finite subgroup of rotations of $O(3, \mathbb{R})$ is isomorphic to one of the following groups:*

$$Z_n, D_{2n}, T, Q, Y.$$

Comment 1. The conditions on the orbits, their lengths, their poles and the order of the group that we obtained are necessary, but it is not clear that they are sufficient for the corresponding finite group of rotations G to exist. In the last three cases, we mentioned that they exist if regular polyhedra in \mathbb{R}^3 exist (those were not rigorously defined). They can be presented by just giving coordinates of their vertices, which is usually sufficient to verify any reasonable definition. After this it can be shown that the groups which appear in each case are unique up to isomorphisms.

Comment 2. Existence of a cube and a regular octahedron are equivalent and easy problems: centers of faces of one of them form the vertex set of another (one is dual of the other).

Existence of regular dodecahedrons and icosahedrons are equivalent and harder problems: centers of faces of one of them form the vertex set of another (one is dual of the other). The following Cartesian coordinates define the vertices of an icosahedron with edge-length 2, centered at the origin:

$$\begin{aligned} &(0, \pm 1, \pm \phi) \\ &(\pm 1, \pm \phi, 0) \\ &(\pm \phi, 0, \pm 1), \end{aligned}$$

where $\phi = (1 + \sqrt{5})/2$ is the golden ratio.

¹¹The image is taken from <http://www.bastiaanluijk.com/>.

Comment 3. Without giving a definition of a convex regular polyhedra in \mathbb{R}^n , we just wish to mention that there are 6 regular polyhedra in \mathbb{R}^4 with 5 being generalizations of the ones in \mathbb{R}^3 , and there are only 3 regular polyhedra in \mathbb{R}^n for $n \geq 5$. The latter are analogs of regular tetrahedron, cube and octahedron in \mathbb{R}^3 . Their complete symmetry groups are examples of finite subgroups of $O(n, \mathbb{R})$.

Lectures 24.

Finite isometry groups containing reflections; Goursat's Lemma.

With understanding of all finite rotation groups of \mathbb{R}^n , $n = 1, 2, 3$, we can now pass to describing all corresponding finite subgroups of the whole $O(n, \mathbb{R})$. It is clear that there exists only one reflection in $O(1, \mathbb{R})$, namely $x \mapsto -x$. Hence, $O(1, \mathbb{R}) \cong \mathbb{Z}_2$. It is easy to argue that every finite subgroup of $O(2, \mathbb{R})$ is either cyclic or dihedral.

Suppose $n = 3$. The map $z : x \mapsto -x$ is a (central) reflection, which is in the center of $O = O(3, \mathbb{R})$. Let Γ be a finite subgroup of O , and let Γ contain a reflection. We consider two cases, depending on whether $z \in \Gamma$ or $z \notin \Gamma$. Let $\Gamma^+ = \Gamma \cap O^+$. If $z \in \Gamma$, then, obviously,

$$\Gamma = \Gamma^+ \cup z\Gamma^+ \cong \Gamma^+ \times \langle z \rangle.$$

If $z \notin \Gamma$, then there exists a reflection $a \in \Gamma$, and so $\Gamma = \Gamma^+ \cup a\Gamma^+$. Suppose $\Gamma^+ = \{g_1, \dots, g_m\}$. For every i , let $t_i = zag_i$. Then t_i is a rotation, and $ag_i = zt_i$. It turns out that

$$\Gamma' = \Gamma^+ \cup \{t_1, \dots, t_m\} = \{g_1, \dots, g_m, t_1, \dots, t_m\}$$

is a group of rotations! The verification is easy: the only thing we have to check is that Γ' is closed under the operation in O . It is indeed. Obviously the product of any two g_i and g_j is in Γ^+ , and so it is in Γ' . Now,

$$t_i t_j = (zag_i)(zag_j) = z^2(ag_i)(ag_j) = (ag_i)(ag_j) \in \Gamma^+,$$

since $\Gamma = \Gamma^+ \cup a\Gamma^+$. Similarly, $t_i g_k = (zag_i)g_k = (za)(g_i g_k)$. As both za and $g_i g_k$ are in Γ^+ , so is $t_i g_k$. It is easy to check (do it) that $\Gamma \cong \Gamma'$, and $g_i \mapsto g_i$, $t_i \mapsto ag_i$ is an isomorphism.

The argument above can be reversed in the following sense. Starting with a finite group of rotations Γ' which contains a subgroup Γ'' of index 2, one can construct a finite subgroup Γ of O containing a reflection, which is isomorphic to Γ' and *not* isomorphic to $\Gamma'' \times \mathbb{Z}_2$. Indeed, let $\Gamma' = \Gamma'' \cup g\Gamma''$. Replace now g with a reflection a of O such $z \notin a\Gamma''$ (why does such exist?!) It is easy to check that $\Gamma'' \cup a\Gamma''$ is a subgroup of O but, obviously, not of O^+ . Since $z \notin a\Gamma''$, then we arrive to a group without a normal subgroup of order 2 (why?).

Denote the group Γ obtained this way as $\Gamma'\Gamma''$. This leads to a complete description of finite subgroups of O . We recall that the groups T of rotations of a regular tetrahedron is a subgroup of index 2 of group Q – the rotation group of a regular octahedron : a good way to see it is by using the fact that midpoints of six edges of a tetrahedron are vertices of an octahedron.

Theorem 36. *Every finite subgroup of $O(3, \mathbb{R})$ containing a reflection is isomorphic to one of the following groups:*

$$\begin{aligned} &Z_n \times \mathbb{Z}_2, D_{2n} \times \mathbb{Z}_2, T \times \mathbb{Z}_2, O \times \mathbb{Z}_2, Y \times \mathbb{Z}_2, \\ &Z_{2n}Z_n, D_{2n} \times \mathbb{Z}_n, D_{4n}D_{2n}, QT. \end{aligned}$$

The study of a relation between finite subgroups of O and O^+ leads to a very interesting question:

how can one characterize all subgroups of the direct $G_1 \times G_2$ if all subgroups of each G_i are known?

It is obvious that if $H_1 \leq G_1$ and $H_2 \leq G_2$, then $H_1 \times H_2 \leq G_1 \times G_2$. On the other hand, it is well known, that these are, in general, not all subgroups of $G_1 \times G_2$. For example, if $G_1 = G_2 = G \neq \langle e \rangle$, then $\{(g, g) : g \in G\} \leq G \times G$, but it is not a direct product of two subgroups of G . The answer to this question is given in the following theorem, known as Goursat's Lemma.

The presentation below is based on the exposition by K. Bauer, D. Sen, P. Zvengrowski in [2].

Let $H \leq G_1 \times G_2$, $\pi_1 : H \rightarrow G_1$ and $\pi_2 : H \rightarrow G_2$ be natural projections, and $\iota_1 : G_1 \rightarrow G_1 \times G_2$ and $\iota_2 : G_2 \rightarrow G_1 \times G_2$ be the usual inclusions. This mean that

$$\pi_1(a, b) = a, \pi_2(a, b) = b, \iota_1(g_1) = (g_1, e_2), \iota_2(g_2) = (e_1, g_2).$$

Theorem 37. (Goursat's Lemma, 1889.) *There is a bijective correspondence between subgroups H of $G_1 \times G_2$ and quintuples $(H_1, \overline{H_1}, H_2, \overline{H_2}, \theta)$, where $H_1 \trianglelefteq \overline{H_1} \leq G_1$, $H_2 \trianglelefteq \overline{H_2} \leq G_2$, and $\theta : \overline{H_1}/H_1 \rightarrow \overline{H_2}/H_2$ is an isomorphism.*

Proof. Define $\overline{H_i}$ as $\pi_i(H)$, and H_i as $\iota_i^{-1}(H)$, $i = 1, 2$. It is easy to check (do it) that $H_i \trianglelefteq \overline{H_i}$. Let $\theta : \overline{H_1}/H_1 \rightarrow \overline{H_2}/H_2$, defined as $\theta(H_1 a) = H_2 b$. It s easy to check (do it) that θ is well-defined and is an isomorphism of groups. Thus H determines the quintuple $\mathcal{H} = (H_1, \overline{H_1}, H_2, \overline{H_2}, \theta)$. Let $\phi : H \mapsto \mathcal{H}$ be a map from the set of subgroups of $G_1 \times G_2$ to the set of the quintuples.

Let us construct the inverse of ϕ , i.e., to prove the converse statement. Consider a quintuple $\mathcal{H} = (H_1, \overline{H_1}, H_2, \overline{H_2}, \theta)$ satisfying the conditions of the theorem. Let $p : \overline{H_1} \times \overline{H_2} \rightarrow \overline{H_1}/H_1 \times \overline{H_2}/H_2$ be the natural surjective homomorphism, and let

$$\mathcal{H}_\theta = \{(H_1 a, \theta(H_1 a)) : a \in \overline{H_1}\} \subseteq \overline{H_1}/H_1 \times \overline{H_2}/H_2$$

be the **graph** of θ . It is easy to check that

$$\mathcal{H}_\theta \leq \overline{H_1}/H_1 \times \overline{H_2}/H_2.$$

Consider $H = p^{-1}(\mathcal{H}_\theta)$, and let $\psi : \mathcal{H} \mapsto H$ define a map from the set of the quintuples to the set of subgroups of $G_1 \times G_2$. It is easy to check that the maps ϕ and ψ are inverses of one another, which completes the proof of the theorem. \square

The proof becomes a bit simpler if each p_i is surjective, i.e., $\pi_i(H) = G_i$. In this case H is called a **subdirect** product of G_1 and G_2 .

Lectures 25.

Finite isometry groups of $GL(n, \mathbb{R})$ and $GL(n, \mathbb{Z})$, $n \geq 1$.

A remarkable theorem of H. Mashke claims that every finite subgroups of $GL(n, \mathbb{R})$ is isomorphic to one of $O(n, \mathbb{R})$. We will explain that this means that every finite group of linear transformations is isomorphic to a group of congruences of the usual Euclidean geometry on \mathbb{R}^n , $n \geq 1$.

Theorem 38. *Every finite subgroup of $GL(n, \mathbb{R})$, is isomorphic to one of $O(n, \mathbb{R})$.*

Proof. Let G be a finite subgroup of $GL(n, \mathbb{R})$, thought as a group of matrices, and let a quadratic form Q on \mathbb{R}^n be defined as

$$Q(x) = \sum_{g \in G} g(x)(g(x))^t,$$

where $(g(x))^t$ represents column vector, and the product $yy^t = \sum_{i=1}^n y_i^2$ is the standard norm in \mathbb{R}^n .

Then for any $h \in G$, $Q(h(x)) = Q(x)$, i.e., Q is invariant with respect to G . It is also clear that Q is positive definite: $Q(x) \geq 0$, and the equality is attained on zero vector only. It is a well-known fact that Q can be reduced to a sum of squares by some non-degenerate linear transformation ϕ , and hence, $\phi^{-1}G\phi$ is a subgroup of the orthogonal group $O(n, \mathbb{R})$. Therefore Theorems 35 and 36 give all isomorphic classes for finite subgroups of $GL(n, \mathbb{R})$. \square

Next we wish to discuss the finite subgroups of $GL(n, \mathbb{Z})$ – the groups of all invertible \mathbb{Z} -linear transformations of \mathbb{Z}^n . As \mathbb{Z}^n can be considered as a discrete analog of \mathbb{R}^n , this group can be thought as a discrete analog of $GL(n, \mathbb{R})$. The description is very surprising.

Theorem 39. *There are finitely many finite subgroups of $GL(n, \mathbb{Z})$, and each of them is isomorphic to a subgroup of $GL(n, \mathbb{F}_p)$ for every odd prime number p .*

Proof. Let p be an odd prime, and let $\phi_p : \mathbb{Z} \rightarrow \mathbb{Z}/(p\mathbb{Z}) = \mathbb{Z}_p = \mathbb{F}_p$ be the canonical homomorphism of the rings sending x to $x + p\mathbb{Z}$. It defines a homomorphism of the matrix groups

$$\overline{\phi}_p : GL(n, \mathbb{Z}) \rightarrow GL(n, \mathbb{F}_p),$$

defined by $A = (a_{ij}) \mapsto \overline{\phi}_p(A) = (\phi_p(a_{ij}))$. In other words, $\overline{\phi}_p(A)$ is a matrix obtained from A by reducing all entries of A modulo p and considering it as an element of $GL(n, \mathbb{F}_p)$ (why is it?). It is clear that the kernel of $\overline{\phi}_p$ consists of all matrices of the form $A = I + pB$, where I is the identity matrix, B and A are integer matrices, and $\det A = \pm 1$. Let us prove that any finite subgroup G of $GL(n, \mathbb{Z})$ is mapped isomorphically by $\overline{\phi}_p$ onto some subgroup of $GL(n, \mathbb{F}_p)$. If we succeed, the theorem is proved, as there are finitely many subgroups of $GL(n, \mathbb{F}_p)$. An estimate on the number of finite subgroups of $GL(n, \mathbb{Z})$, as well as restrictions on their orders, can be obtained from a well-known formula

$$|GL(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).$$

The kernel of $\overline{\phi}_p$ restricted on G is the intersection G and $\text{Ker}(\overline{\phi}_p)$. Therefore if we show that $\text{Ker}(\overline{\phi}_p)$ has no elements of finite order different from I , we are

done. Let $A = I + p^r B$, where B is an integer matrix such that not every entry of B is divisible by p . If $A^n = I$, then, using the binomial theorem, we obtain

$$np^r B + \sum_{k=2}^n \binom{n}{k} p^{rk} B^k = 0.$$

It is easy to show that for $p > 2$ and $k \geq 2$, some entries of the matrix $\sum_{k=2}^n \binom{n}{k} p^{rk} B^k$ are divisible by a bigger power of p than the corresponding entries of the matrix $np^r B$ (show this!). The obtained contradiction proves that no nonidentity matrix in $\text{Ker}(\overline{\phi_p})$ is of finite order. Hence, $\overline{\phi_p}$ restricted on G is an injection, and the theorem is proved. \square

REFERENCES

- [1] M. Artin, Algebra : applications, and Algorithms, 2nd edition, Prentice Hall, 2011.
- [2] K. Bauer, D. Sen, P. Zvengrowski in *A generalized Goursat Lemma*, arXiv:1109.0024v2 [math.GR], http://arxiv.org/PS_cache/arxiv/pdf/1109/1109.0024v2.pdf.
- [3] K. Conrad, Groups of order p^3 , <http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/groupsp3.pdf>
- [4] D.S. Dummit, R.M. Foote, Abstract Algebra, 3rd edition, John Willey & Sons, 2004.
- [5] M. Hall, Jr., Theory of Groups, The Macmillian Company, New York, 1959.
- [6] N. Jacobson, Basic Algebra 1, W.H. Freeman and Company, 1974.
- [7] M.I. Kargapolov, J.I. Merzljakov, Fundamentals of the theory of groups , Springer, 1979.
- [8] G. Jones, M.H. Klin, F. Lazebnik, Introduction to the Theory of Automorphic Subsets of the n -dimensional Cube, *Beitrge zur Algebra und Geometrie, (Contributions to Algebra and Geometry,)* Volume 41 (2000), No.2, 303–323. The article can also be seen as <http://www.emis.de/journals/BAG/vol.41/no.2/b41h2k1i.pdf>
- [9] A.I. Kostrikin, I.R. Shafarevich, Algebra 1 : Basic Notions of Algebra, Encyclopaedia of Mathematical Sciences, Springer-Verlag, 1990.
- [10] S. Lang, Algebra, 3rd ed., Addison-Wesley Publishing Company, Inc., 1993.
- [11] E.B. Vinberg, A Course in Algebra, Graduate Studies in Mathematics, Volume 56, American Mathematical Society, 2003.
- [12] H. Weyl, Symmetry, Princeton Universty Press, 1952.