ЗАКАРПАТСЬКИЙ УГОРСЬКИЙ ІНСТИТУТ ІМЕНІ ФЕРЕНЦА РАКОЦІ ІІ
II. RÁKÓCZI FERENC KÁRPÁTALJAI MAGYAR FŐISKOLA

Кафедра математики та інформатики
Matematika és Informatika Tanszék

«ADDITIONAL TOPICS IN CONTEMPORARY MATHEMATICS»
(КУРС ЛЕКЦІЙ)

(для студентів 2-го курсу спеціальності 014 Середня освіта (Математика))

ADDITIONAL TOPICS IN CONTEMPORARY MATHEMATICS

Другий (магістерський) / Mesterképzés (MA)
(ступінь вищої освіти /a felsőoktatás szintje)

01 Освіта/Педагогіка */ 01 Oktatás/Pedagógia*
(галузь знань / képzési ág)

"Середня освіта (*Математика*)*"*
"Középfokú oktatás (*Matematika*)*"*
(освітня програма / képzési program)

Берегове / Beregszász
2024 р. / 2024

Посібник з додаткових розділів сучасної математики призначений для студентів ІІ курсу (ступеня магістра) Закарпатського угорського інституту імені Ференца Ракоці спеціальності 014 Середня освіта (математика) денної та заочної форми навчання з метою організації лекційного курсу "Додаткові розділи сучасної математики".

Посібник поділений на розділи, кожен з яких містить теоретичні відомості певної математичної структури. Посібник викладений англійською мовою.

Матеріал призначений для використання як навчально-методичний посібник з дисципліни "Додаткові розділи сучасної математики".

Затверджено до використання у навчальному процесі
на засіданні кафедри математики та інформатики
(протокол № 1 від «13» серпня 2024 року)

Розглянуто та рекомендовано Радою із забезпечення якості освіти
Закарпатського угорського інституту імені Ференца Ракоці ІІ
(протокол № 22 від «26» серпня 2024 року)

Рекомендовано до видання у електронній формі (PDF)
рішенням Вченої ради Закарпатського угорського інституту імені Ференца Ракоці ІІ
(протокол № 7 від «27» серпня 2024 року)

Підготовлено до видання у електронній формі (PDF) кафедрою математики та інформатики з Видавничим відділом Закарпатського угорського інституту імені Ференца Ракоці ІІ

Укладач:

СТОЙКА МИРОСЛАВ ВІКТОРОВИЧ – доцент кафедри математики та інформатики Закарпатського угорського інституту імені Ференца Ракоці ІІ

Рецензенти:

СЛИВКА НАТАЛІЯ ТЕОДОРІВНА –старший викладач кафедри іноземних мов факультету іноземної філології ДВНЗ «УжНУ»;
БОРТОШ МАРІЯ ЮЛІЇВНА – кандидат фізико-математичних наук, доцент кафедри алгебри та диференціальних рівнянь ДВНЗ «УжНУ»;
МЕСАРОШ ЛІВІА ВАСИЛІВНА– кандидат фізико-математичних наук, доцент кафедри математики та інформатики ЗУІ.

Відповідальний за випуск:

Олександр ДОБОШ – начальник Видавничого відділу ЗУІ ім. Ф.Ракоці ІІ

За зміст посібника відповідальність несуть розробники.

Видавництво: Закарпатський угорський інститут імені Ференца Ракоці ІІ (адреса: пл. Кошута 6, м. Берегове, 90202. Електронна пошта: foiskola@kmf.uz.ua)

Az ADDITIONAL TOPICS IN CONTEMPORARY MATHEMATICS a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola, az MSc szint II. éves, matematika szakos, nappali és levelező hallgatóinak készült, a Korszerű matematika válogatott fejezetei c. tantárgy alaposabb tanulmányozásának és elsajátításának megkönnyítése céljából.

Ez a jegyzet elsősorban matematika szakos hallgatók számára készült, de hasznos lehet mindazok számára, akik bármely más szakon tanulnak matematikát.

A jegyzet fejezetekre van osztva. Minden fejezetben röviden egy téma let kidolgozva, melyben általában fogalmak és alapelvek vannak bemutatva angol nyelven.

Az oktatási folyamatban történő felhasználását jóváhagyta
a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
Matematika és Informatika Tanszéke
(2024. augusztus 13, 1. számú jegyzőkönyv).

Megjelentetésre javasolta a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
Minőségbiztosítási Tanácsa
(2024. augustzus 26 , 22. számú jegyzőkönyv).

Elektronikus formában (PDF fájlformátumban) történő kiadásra javasolta
a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Tudományos Tanácsa
(2024. augustzus 27 , 7. számú jegyzőkönyv).

Kiadásra előkészítette a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
Matematika és Informatika Tanszéke és Kiadói Részlege.

Szerkesztő:

SZTOJKA MIROSZLÁV – a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Matematika és Informatika Tanszékének docense

Szakmai lektorok:

SZLIVKA NATÁLIA – Ungvári Nemzeti Egyetem Idegennyelvi Tanszékének adjunktusa;

BARTOS MÁRIA – fizika és matematika tudományok kandidátusa, docens, az Ungvári Nemzeti Egyetem Algebra és Diferenciál Egyenletek Tanszékének docense;

MÉSZÁROS LÍVIA – fizika és matematika tudományok kandidátusa, II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Matematika és Informatika Tanszékének docense.

A kiadásért felel:

DOBOS Sándor – a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Kiadói Részlegének vezetője

A tartalomért kizárólag a jegyzet szerkesztője felel.

Kiadó: a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola (cím: 90 202, Beregszász, Kossuth tér 6. E-mail: foiskola@kmf.uz.ua)

Contents

1. Group Theory

Definition of a Group

A group is an algebraic structure consisting of a set G and a binary operation $*$ defined on G. This structure satisfies the following four axioms:

1. Associativity: For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

2. Existence of an Identity Element: There exists an element e in G such that for all $a \in G, a * e = e * a = a$.

3. Existence of an Inverse Element: For each element a in G, there exists an element a^{-1} in G such that $a * a^{-1} = a^{-1} * a = e$, where e is the identity element.

4. Commutativity (for Abelian groups): If the operation $*$ is commutative, i.e., for all a, b in G, $a * b = b * a$, then the group is called Abelian.

Examples of Groups

1. The Set of Integers $\mathbb{Z}$ under Addition: The set $\mathbb{Z}$ with the operation of addition forms an Abelian group, where the identity element is 0, and the inverse element for any a is $-a$.

2. The Set of Non-Zero Rational Numbers $\mathbb{Q}^*$ under Multiplication$*$: The set $\mathbb{Q}^*$ forms an Abelian group, where the identity element is 1, and the inverse element for any q is $\frac{1}{q}$.

3. Symmetric Group: For the set $\{1, 2, 3, \ldots, n\}$, the symmetric group S_n consists of all possible permutations of this set. It is a non-Abelian group, where the operation is the composition of permutations.

Subgroups

A subset $H \subseteq G$ is called a subgroup of a group G if H itself is a group with the same operation as in G. This requires that for all $a, b \in H$, the elements $a * b$ and a^{-1} are also in H.

Cyclic Groups

A group G is called cyclic if there exists an element g in G such that every element of the group can be expressed as a power of g, i.e., for each a in G, there exists an integer n such that $a = g^n$. The element g is called the generator of the group.

Lagrange's Theorem

For a finite group G, if H is a subgroup of G, then the order (number of elements) of the subgroup H divides the order of the group G.

This theorem is one of the central results in group theory and has many important implications in various fields of mathematics.

Group Homomorphisms

A homomorphism from a group G to a group H is a map $\varphi: G \to H$ that preserves the group operation, i.e., for all a, b in G, $\varphi(a * b) = \varphi(a) * \varphi(b)$. If the homomorphism φ is bijective, it is called an isomorphism, and the groups G and H are said to be isomorphic.

Applications of Group Theory

Group theory is widely used in various fields of mathematics, physics, and computer science. It helps in analyzing symmetries in geometric objects, structures in algebraic systems, and plays a key role in number theory and cryptography.

2. Ring Theory

Ring theory is a branch of abstract algebra that studies rings, which are algebraic structures equipped with two binary operations: addition and multiplication. A ring R is defined as a set equipped with two operations that satisfy the following properties:

1. Addition: The set R is closed under addition, meaning that for any two elements $a, b \in R$, the sum $a + b$ is also in R. Additionally, addition in R must satisfy the following properties:

- Associativity: $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.
- Commutativity: $a + b = b + a$ for all $a, b \in R$.
- Identity Element: There exists an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$.
- Additive Inverse: For each $a \in R$, there exists an element $-a \in R$ such that $a + (-a) = 0$.

2. Multiplication: The set R is closed under multiplication, meaning that for any two elements $a, b \in R$, the product $a \cdot b$ is also in R. Multiplication in R must satisfy the following properties:

- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

- Distributivity: Multiplication is distributive over addition; that is, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

A ring is called commutative if multiplication is commutative, i.e., $a \cdot b = b \cdot a$ for all $a, b \in R$.

Examples of Rings

- The set of integers $\mathbb{Z}$ with the usual addition and multiplication is a commutative ring.
- The set of $n \times n$ matrices with real entries is a non-commutative ring.

Subrings and Ideals

- A subring of a ring R is a subset of R that is itself a ring with the inherited operations from R.

- An ideal of a ring R is a subring I such that for every $r \in R$ and $i \in I$, both $r \cdot i$ and $i \cdot r$ are in I.

Ring Homomorphisms

A ring homomorphism is a function $f: R \to S$ between two rings R and S that preserves the ring operations, meaning:

- $f(a + b) = f(a) + f(b)$ for all $a, b \in R$,

- $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in R$,

$-$ $f(1_R) = 1_S$ if R and S have multiplicative identities.

3. Field Theory

Field theory is a branch of algebra that studies fields, which are algebraic structures with two operations: addition and multiplication. A field F is a set equipped with two operations that satisfy the following properties:

1. **Addition**:

- Closure: For any two elements $a, b \in F$, their sum $a + b$ is also in F.

- Associativity: $(a + b) + c = a + (b + c)$ for all $a, b, c \in F$.

- Commutativity: $a + b = b + a$ for all $a, b \in F$.

- Identity Element: There exists an element $0 \in F$ such that $a + 0 = a$ for all $a \in F$.

- Additive Inverse: For each $a \in F$, there exists an element $-a \in F$ such that $a + (-a) = 0$.

2. **Multiplication**:

- Closure: For any two elements $a, b \in F$, their product $a \cdot b$ is also in F.

- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in F$.

- Commutativity: $a \cdot b = b \cdot a$ for all $a, b \in F$.

- Identity Element: There exists an element $1 \in F$ (where $1 \neq 0$) such that $a \cdot 1 = a$ for all $a \in F$.

- Multiplicative Inverse: For each $a \in F$ (where $a \neq 0$), there exists an element $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$.

3. Distributivity:

- Multiplication is distributive over addition; that is, $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

Examples of Fields

- The set of rational numbers $\mathbb{Q}$ with the usual addition and multiplication is a field.
- The set of real numbers $\mathbb{R}$ and the set of complex numbers $\mathbb{C}$ are also fields.

Subfields and Extensions

- A subfield of a field F is a subset of F that is itself a field with the inherited operations from F.

- A field extension is a larger field E containing a subfield F. The study of field extensions often involves analyzing the degree of the extension, which is the dimension of E as a vector space over F.

Field Homomorphisms

A field homomorphism is a function $f: F \rightarrow G$ between two fields F and G that preserves the field operations, meaning:

- $f(a + b) = f(a) + f(b)$ for all $a, b \in F$,
- $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in F$,
- $f(1_F) = 1_G$, where 1_F and 1_G are the multiplicative identities of F and G, respectively.

4. Module Theory

Modules are a fundamental concept in abstract algebra, serving as a generalization of vector spaces over a field. While vector spaces are defined over fields, modules are defined over rings, allowing for a broader range of algebraic structures. The theory of modules provides a framework for studying linear algebra in a more generalized context, where the scalar multiplication is not restricted to fields but can be extended to rings.

A **module** over a ring R (with unity) is an abelian group M equipped with a binary operation called scalar multiplication that associates each element $r \in R$ r and each element $m \in M$ with an element $rm \in M$. The operation satisfies the following axioms for all $r, s \in R$ and $m, n \in M$:

1. **Distributivity over ring addition:** $r(m + n) = rm + rn$
2. **Distributivity over module addition:** $(r + s)m = rm + sm$
3. **Associativity:** $(rs)m = r(sm)$
4. **Unity:** $1_R m = m1_R$, where 1_R is the multiplicative identity in R.

Examples of Modules

- **Vector Spaces:** Every vector space is a module where the ring R is a field.
- **Abelian Groups** as $\mathbb{Z}$**-**Modules**:** Any abelian group can be viewed as a module over the ring of integers $\mathbb{Z}$.
- **Matrices as Modules:** The set of all $m \times n$ matrices over a ring R forms a module over R.

Submodules

A **submodule** of a module M over a ring R is a subset N of M that is closed under addition and scalar multiplication. In other words, N is a submodule if for all $m, n \in N$ and $r \in R$:

- $m + n \in N$
- $rm \in N$

Submodules are analogous to subspaces in vector space theory.

Quotient Modules

Given a module M over a ring R and a submodule N of M, the **quotient module** M/N is defined as the set of cosets of N in M. The operations on M/N are defined as follows:

- $(m + N) + (n + N) = (m + n) + N$
- $r(m + N) = (rm) + N$

The quotient module M/N inherits the module structure from M.

Homomorphisms and Isomorphisms

A **module homomorphism** between two R-modules M and N is a function $f: M \to N$ that preserves the module operations:

- $f(m + n) = f(m) + f(n)$ for all $m, n \in M$
- $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$

An isomorphism is a bijective homomorphism, meaning that the two modules are structurally identical.

Exact Sequences

An **exact sequence** of modules is a sequence of module homomorphisms:

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} \cdots \xrightarrow{f_{n-1}} M_n$$

that satisfies the condition that the image of each homomorphism is equal to the kernel of the next:

$$\mathrm{Im}(f_i) = \ker(f_{i+1})$$

Exact sequences are a key concept in module theory and are used extensively in homological algebra.

Projective, Injective, and Free Modules

- **Projective Modules:** A module P is projective if every surjective module homomorphism onto P splits.
- **Injective Modules:** A module Q is injective if every injective module homomorphism from Q can be extended.
- **Free Modules:** A module is free if it has a basis, meaning it is isomorphic to a direct sum of copies of the ring R.

5. Galois Theory

Galois Theory is a branch of abstract algebra that connects field theory with group theory, providing profound insights into the solvability of polynomial equations. Named after the French mathematician Évariste Galois, this theory establishes a correspondence between field extensions and groups, allowing mathematicians to understand the roots of polynomials and their symmetries in a structured way.

Field Extensions

A **field extension** is a pair of fields E and F such that $F \subseteq E$. The field E is called an extension of F, and F is called the base field. The degree of the extension E over F, denoted by $[E:F]$, is the dimension of E as a vector space over F.

- **Example:** The field $\mathbb{C}$ of complex numbers is an extension of the field $\mathbb{R}$ of real numbers, and the degree of the extension is $[C:R] = 2$.

Galois Extensions

A field extension E of F is called a Galois extension if it is both normal and separable.

- Normality: An extension E is normal over F if every irreducible polynomial in $F[x]$ that has a root in E completely factors into linear factors over E.
- Separability: An extension E is separable over F if every element of E is a root of a separable polynomial over F (a polynomial whose roots are distinct).

Galois Group

The Galois group of a field extension E over F, denoted $\mathrm{Gal}(E/F)$, is the group of all field automorphisms of E that fix F. In other words, it consists of all the bijective maps $\sigma: E \to E$ such that σ(a)=a for all $a \in F$.

- **Example:** For the extension $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) / \mathbb{Q})$has two elements: the identity map and the automorphism that sends $\sqrt{2}$ to $-\sqrt{2}$.

Fundamental Theorem of Galois Theory

The **Fundamental Theorem of Galois Theory** states that there is a one-to-one correspondence between the intermediate fields $F \subseteq K \subseteq E$ and the subgroups of the Galois group $\mathrm{Gal}(E/F)$. This correspondence reverses inclusions:

- If K is an intermediate field, then its corresponding subgroup is $\mathrm{Gal}(E/K)$.
- If H is a subgroup of $\mathrm{Gal}(E/F)$, then the corresponding intermediate field is the fixed field E^H, consisting of elements in E that are fixed by all automorphisms in H.

Solvability by Radicals

One of the most famous applications of Galois Theory is determining whether a polynomial equation can be solved by radicals (i.e., solutions can be expressed using a finite number of operations involving addition, subtraction, multiplication, division, and root extraction). A polynomial is solvable by radicals if and only if its Galois group is a solvable group.

Applications of Galois Theory

Galois Theory has far-reaching applications in various fields of mathematics:

- **Classical Problems:** Galois Theory provides solutions to classical problems such as the impossibility of trisecting an angle or doubling a cube using only a compass and straightedge.
- **Algebraic Number Theory:** It plays a crucial role in the study of algebraic number fields and their ring of integers.

- **Cryptography:** The theory also has applications in modern cryptography, particularly in the design of certain cryptographic protocols based on finite fields.

Galois Theory bridges the gap between field theory and group theory, providing deep insights into the structure of polynomials and their roots. It offers powerful tools for understanding the solvability of equations and has significant implications across various areas of mathematics.

6. Quaternion Theory

Quaternions are an extension of complex numbers, introduced by Sir William Rowan Hamilton in 1843. They provide a way to represent rotations in three-dimensional space and are used in various applications such as computer graphics, robotics, and physics. Quaternions extend the concept of two-dimensional complex numbers to four dimensions and are expressed in the form:

$$q = a + bi + cj + dk$$

where $a, b, c,$ and d are real numbers, and $i, j,$ and k are the fundamental quaternion units.

Quaternion Algebra

The fundamental quaternion units $i, j,$ and k satisfy the following multiplication rules:

$$i^2 = j^2 = k^2 = ijk = -1$$
$$ij = k, ji = -k$$
$$jk = i, kj = -i$$
$$ki = j, ik = -j$$

These relations show that quaternion multiplication is non-commutative, meaning that the order of multiplication matters.

Quaternion Conjugate and Norm

The **conjugate** of a quaternion $q = a + bi + cj + dk$ is given by:

$$\bar{q} = a - bi - cj - dk$$

The **norm** of a quaternion q is defined as:

$$| q | = \sqrt{a^2 + b^2 + c^2 + d^2}$$

The norm of a quaternion is always a non-negative real number.

Quaternion Inverse

The inverse of a non-zero quaternion q is given by:

$$q^{-1} = \frac{\bar{q}}{| q |^2}$$

Multiplying a quaternion by its inverse yields the multiplicative identity quaternion, $1 + 0i + 0j + 0k$.

Quaternions and Rotations

Quaternions are particularly useful in representing rotations in three-dimensional space. A rotation by an angle θ around a unit vector $u = (u_1, u_2, u_3)$ can be represented by the quaternion:

$$q = \cos\left(\frac{\theta}{2}\right) + \sin\left(\frac{\theta}{2}\right)(u_1 i + u_2 j + u_3 k)$$

To rotate a vector v using the quaternion q, we use the operation:

$$v' = qvq^{-1}$$

where v' is the rotated vector.

Applications of Quaternions

Quaternions have several important applications in various fields:

- **Computer Graphics:** Quaternions are used to represent and interpolate rotations, avoiding the problems of gimbal lock and providing smooth transitions between orientations.
- **Robotics:** Quaternions are used to control the orientation of robotic arms and other mechanical systems.

- **Physics:** In quantum mechanics and relativity, quaternions are used to describe the spin and orientation of particles.

Quaternions extend complex numbers into four dimensions and provide a powerful framework for representing rotations in three-dimensional space. Their non-commutative nature and unique algebraic properties make them an essential tool in mathematics, physics, and engineering.

7. Group Ring Theory

Group rings are a significant concept in algebra that arise from the interaction between group theory and ring theory. Given a group G and a ring R, the group ring $R[G]$ is a construction that allows the combination of elements of G with coefficients from R. This construction plays a crucial role in various areas of mathematics, including representation theory, homological algebra, and number theory.

Definition of Group Rings

Let G be a group and R be a ring. The group ring $R[G]$ consists of all finite formal sums:

$$\sum_{g \in G} \alpha_g \, g$$

where $\alpha_g \in R$ for each $g \in G$, and only finitely many α_g are non-zero. The addition and multiplication in $R[G]$ are defined as follows:

- **Addition:**

$$\sum_{g \in G} \alpha_g \, g + \sum_{g \in G} \beta_g \, g = \sum_{g \in G} (\alpha_g + \beta_g) \, g$$

- **Multiplication:**

$$\left(\sum_{g \in G} \alpha_g \, g \right) \cdot \left(\sum_{h \in G} \beta_h \, h \right) = \sum_{g,h \in G} (\alpha_g \beta_h) \, (gh)$$

Here, the product gh denotes the group operation in G, and $\alpha_g \beta_h$ denotes the product in the ring R.

Examples of Group Rings

- **Example 1:** Consider the group $G = \mathbb{Z}_2 = \{1, -1\}$ and the ring $R = \mathbb{Z}$ (the integers). The group ring $\mathbb{Z}[\mathbb{Z}_2]$ consists of elements of the form $a \cdot 1 + b \cdot (-1)$, where $a, b \in \mathbb{Z}$.
- **Example 2:** If G is the group of permutations on n elements, S_n, and $R = \mathbb{R}$ (the real numbers), then $\mathbb{R}[S_n]$ is the group ring of the symmetric group.

Properties of Group Rings

Group rings inherit various properties from both the group G and the ring R:

- **Associativity:** The group ring $R[G]$ is associative since both the group operation in G and the multiplication in R are associative.
- **Distributivity:** The distributive property holds in $R[G]$, allowing the multiplication of elements to distribute over addition.
- **Identity Element:** If R has an identity element, then $R[G]$ also has an identity element, which is the group identity element multiplied by the ring identity.

Applications of Group Rings

Group rings have numerous applications in various fields:

- **Representation Theory:** Group rings are essential in the study of representations of groups, where they provide a framework for analyzing group actions on vector spaces.
- **Homological Algebra:** In homological algebra, group rings are used to define modules and study their homological properties.
- **Number Theory:** Group rings appear in number theory, particularly in the study of cyclotomic fields and Galois modules.

Group rings serve as a bridge between group theory and ring theory, providing a rich structure that is utilized in many branches of mathematics. Their versatility and broad applicability make them an important topic of study in algebra.

8. Group Representation Theory

Group representation theory is a branch of mathematics that studies abstract groups by representing their elements as linear transformations of vector spaces. This approach allows the use of linear algebra to investigate and understand group properties, making it a powerful tool in both pure and applied mathematics, including physics, chemistry, and computer science.

Definition of Group Representations

A **group representation** of a group G on a vector space V over a field F is a homomorphism $\rho: G \to GL(V)$, where $GL(V)$ is the general linear group of invertible linear transformations of V. In other words, for each element $g \in G$, the representation assigns a linear transformation $\rho(g): V \to V$ such that:

$$\rho(gh) = \rho(g) \cdot \rho(h) \text{ for all } g, h \in G,$$
$$\rho(e) = I_V,$$

where $\boldsymbol{e}$ is the identity element of G and I_V is the identity transformation on V.

Examples of Group Representations

- **Example 1:** Consider the cyclic group $G = \mathbb{Z}_3 = \{0,1,2\}$ under addition modulo 3. A representation of $\mathbb{Z}_3$ on $\mathbb{R}^2$ could be given by rotation matrices corresponding to angles 0°, 120°, and 240°.
- **Example 2:** The symmetric group S_n, which consists of all permutations of n elements, has a natural representation on an n-dimensional vector space by permuting the coordinates of vectors.

Types of Group Representations

- **Irreducible Representations:** A representation ρ is called **irreducible** if the only subspaces of V that are invariant under all $\rho(g)$ for $g \in G$ are $\{0\}$ and V

itself. Irreducible representations are the building blocks of all representations, analogous to prime numbers in number theory.

- **Unitary Representations:** A representation is called **unitary** if $\rho(g)$ is a unitary operator for every $g \in G$. Unitary representations are important in physics, particularly in quantum mechanics.
- **Permutation Representations:** A representation derived from the action of G on a set X by permuting its elements. These are particularly useful in studying symmetries and combinatorial structures.

Characters of Group Representations

The **character** of a group representation ρ is a function $\chi_\rho: G \to F$ defined by:

$$\chi_\rho(g) = \mathrm{Tr}(\rho(g)),$$

where Tr denotes the trace of the linear transformation $\rho(g)$. Characters are a crucial tool in studying representations, as they provide significant information about the structure of the representation.

Applications of Group Representations

Group representations have a wide range of applications across various fields:

- **Physics:** Group representations are used to describe the symmetries of physical systems, particularly in quantum mechanics and particle physics.
- **Chemistry:** Molecular symmetries can be analyzed using group representations, aiding in the understanding of chemical bonding and spectroscopy.
- **Cryptography:** Representations of groups play a role in the study of cryptographic algorithms, particularly in areas like error-correcting codes and public-key cryptography.

Group representation theory provides a bridge between abstract algebra and linear algebra, offering a robust framework for understanding the structure and behavior of groups. Its applications in various scientific disciplines underscore its importance and utility in both theoretical and practical contexts.

9. Matrix Representations of Groups

Matrix representations of groups are a specific type of group representation where the elements of a group are represented as matrices. This approach allows us to apply the tools of linear algebra to study group structures and their properties. Matrix representations are fundamental in various areas of mathematics and physics, especially in quantum mechanics, crystallography, and the theory of symmetry.

Definition of Matrix Representations

A **matrix representation** of a group G on a vector space V over a field F is a homomorphism $\rho: G \to GL_n(F)$, where $GL_n(F)$ is the general linear group of $n \times n$ invertible matrices over F. This means that each element $g \in G$ is associated with an invertible matrix $\rho(g)$ such that:

$$\rho(gh) = \rho(g) \cdot \rho(h) \text{for all } g, h \in G,$$
$$\rho(e) = I_n,$$

where e is the identity element of G and I_n is the $n \times n$ identity matrix.

Examples of Matrix Representations

- **Example 1:** Consider the cyclic group $G = \mathbb{Z}_2 = \{0,1\}$. A matrix representation of $\mathbb{Z}_2$ over $\mathbb{R}$ could be given by the matrices:

$$\rho(0) = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \rho(1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- **Example 2:** The symmetric group S_3, which consists of all permutations of three elements, has a standard matrix representation on $\mathbb{R}^3$ by permuting the coordinates of vectors.

Properties of Matrix Representations

Matrix representations inherit the properties of the underlying group:

- **Linearity:** The homomorphism ρ preserves the group operation, allowing the multiplication of matrices to reflect the group operation.
- **Invertibility:** Since each $\rho(g)$ is an element of $GL_n(F)$, it is invertible, meaning each group element corresponds to an invertible matrix.
- **Dimension:** The dimension of the matrix representation is determined by the size of the matrices, which corresponds to the dimension of the vector space V.

Applications of Matrix Representations

Matrix representations are essential in many scientific and mathematical fields:

- **Physics:** In quantum mechanics, matrix representations of groups describe the symmetries of physical systems, such as rotations and reflections.
- **Chemistry:** Molecular symmetries can be represented using matrix representations, which are crucial in understanding chemical bonding and molecular vibrations.
- **Computer Science:** In computer graphics, matrix representations are used to model transformations, including rotations, translations, and scaling.

Matrix representations provide a concrete and computationally effective way to study group structures through linear algebra. Their applications extend across various disciplines, making them a central concept in both theoretical and applied mathematics.

References

1. Ван Дер Варден, Б.Л. Алгебра. М.: Наука. 1976. 648 с.
2. Пилипів В.М. Теорія представлень груп та її застосування: навч. посібник. Івано-Франківськ: ВДВ ЦІТ Прикарпатського нац. ун-ту, 2008. – 156 с.
3. Холл М. Теория групп. М. : ИЛ, 1962. 468 с.
4. Morris Newman Matrix Representations of Groups. Institute of Basic Standards, U.S. Government Printing Office. 1968. P. 80.