МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
РІВНЕНСЬКИЙ ДЕРЖАВНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Кафедра вищої математики

Б.П. Петрівський, О.А. Рудюк

ОГЛЯДОВІ ЛЕКЦІЇ З АЛГЕБРИ І ТЕОРІЇ ЧИСЕЛ

Рівне - 2009

Посібник містить курс оглядових лекцій з алгебри і теорії чисел для підготовки до державних екзаменів бакалаврату.

Рецензенти: кандидат фізико-математичних наук,
професор кафедри економічної кібернетики Крайчук О.В.
Кандидат фізико - математичних наук,
доцент кафедри вищої математики Марач В.С.

Рекомендовано до друку на засіданні кафедри вищої математики, протокол №6 від 13 січня 2009р.
та на засіданні науково - методичної Ради РДГУ,
протокол №3 від 12 лютого 2009р.

Комп’ютерний набір: Рудюк О.А.

Комп’ютерна верстка: Рудюк О.А.

© Б.П. Петрівський, О.А. Рудюк, 2009

ВСТУП

Посібник призначено для студентів стаціонарних і заочних відділів факультету математики та інформатики та фізико-математичних факультетів педагогічних інститутів. Він містить весь матеріал, передбачений діючою програмою з алгебри і теорії чисел та лінійною алгеброю державного екзамену з математики та методики викладання математики.

В посібнику викладено матеріал 30 лекцій. Структура цих лекцій така: спочатку висвітлено відповідь на тему лекції, відтак можливі додаткові запитання, приклади розв’язання задач, список використаної літератури.

Основна мета посібника допомогти студентам IV курсу більш якісніше підготуватись до державних екзаменів.

В посібнику відображені нові вимоги, які необхідні для підготовки вчителів математики.

Лекція 1. Бінарні відношення. Рефлексивні, симетричні, транзитивні бінарні відношення. Розбиття на класи. Фактор-множина

<u>Означення 1.</u> Прямим добутком двох множин A, B називається множина всіх впорядкованих пар елементів a, b таких, що $a \in A$ і $b \in B$ і позначається $A \times B$.

Таким чином, $A \times B = \{<a, b>: a \in A \wedge b \in B\}$. Якщо, наприклад, $A=\{1,2\}$, $B=\{3,4\}$, то $A \times B=\{<1,3>, <1,4>, <2,3>, <2,4>\}$, $B \times A=\{<3, 1>, <3, 2>, <4,1>, <4, 2>\}$. З цього прикладу випливає, що $A \times B \neq B \times A$.

<u>Означення 2.</u> Бінарним відношенням між елементами множини A і B називається будь-яка підмножина прямого добутку $A \times B$.

Бінарні відношення прийнято позначати малими грецькими буквами. Якщо елементи a, b перебувають у бінарному відношенні α, то це позначають так $<a, b> \in \alpha$ або $a \ \alpha \ b$.

В наведеному вище прикладі можна розглядати 16 (2^4) різних бінарних відношень.

Як правило бінарні відношення задаються на множині істинності певних предикатів. Визначимо в наведеному прикладі предикат $\varphi(\xi,\eta)=$"η**ξ". Зрозуміло, що він приймає істині значення для пар $<1,3>$, $<1,4>$, $<2, 4>$, сукупність яких і є одним з бінарних відношень. Бінарні відношення, які визначені на скінченних множинах, можна задавати переліком елементів, за допомогою таблиць, стрілок, графіком, графом, характеристичною властивістю.

Бінарне відношення еквівалентності визначають, як правило, на одній множині, тобто, розглядають прямий добуток $A \times A$.

<u>Означення 3.</u> Бінарне відношення $\alpha \in A \times A$ називається відношення еквівалентності, якщо воно:

1. рефлексивне, тобто $(\forall a)$ $(<a, a> \in \alpha)$;
2. симетричне, тобто $(\forall a, b)$ $(<a, b> \in \alpha \Rightarrow <b, a> \in \alpha)$;

3. транзитивне, тобто $(\forall a, b, c)\ (\langle a, b\rangle \in \alpha \wedge \langle b, c\rangle \in \alpha \Rightarrow \langle a, c\rangle \in \alpha)$.

Очевидно, що $\alpha = A \times A$ є відношення еквівалентності.

Відношеннями еквівалентності будуть:

1. відношення подібності трикутників на множині всіх трикутників площини;

2. відношення рівнопотужності в довільній множині скінченних множин;

3. відношення рівності;

4. відношення α, яке є значенням істинності предиката “мати однакове прізвище”, на множині жителів міста Рівне.

Взагалі для визначення того, чи буде бінарне відношення α відношенням еквівалентності потрібно перевірити виконання вимог 1, 2, 3 означення 3.

<u>Означення 4</u>. Сукупність S непорожніх підмножин множини A називають розбиттям множини A, якщо кожний її елемент належить одній і тільки одній підмножині з S.

Кожна непорожня множина A завжди має два тривіальні розбиття: поелементне і ціле розбиття.

Нехай α - будь-яке відношення еквівалентності з $A \times A$.

<u>Означення 5</u>. Сукупність всіх елементів $x \in A$, які знаходяться у відношенні α з елементом а називається класом еквівалентності і позначається $[a]$.

Таким чином, $[a]=\{x \in A: \langle x, a\rangle \in \alpha\}$. З означення 5 випливають так дві властивості:

<u>Властивість 1.</u> Кожний елемент $a \in A$ належить своєму класу еквівалентності $[a]$ (це випливає з рефлексивності α).

<u>Властивість 2</u>. Різні класи еквівалентності не перетинаються.

Доведення проведемо методом від супротивного, використовуючи модифікацію $A \Rightarrow B \equiv A \wedge \overline{B} \Rightarrow \overline{A}$.

Припустимо, що різні класи еквівалентності $[a]$, $[b]$ перетинаються і c їх спільний елемент, тобто $c \in [a]$ і $c \in [b]$. Покажемо, що $[a]=[b]$.

Нехай $x \in [a]$. Тоді $<x,a> \in \alpha$ і так як $<a,c> \in \alpha$, то $<x,c> \in \alpha$. Оскільки $<x,c> \in \alpha$, то $<x,b> \in \alpha$. Це означає, що $x \in [b]$ або $[a] \subseteq [b]$. Аналогічно показуємо, що $[b] \subseteq [a]$. Звідси слідує, що $[a]=[b]$.

<u>Означення 6</u>. Сукупність усіх класів еквівалентності множини A за відношенням еквівалентності α називається фактор-множиною і позначається A/α.

Наприклад. Фактор-множина від $A=Z$ за відношенням еквівалентності $\alpha=\{<x,y>: (x-y)**3\}$ є $A\backslash\alpha=\{\{3к\},\{3к+1\}, \{3к+2\}: к \in Z\}$.

Додаткові запитання:

1. Побудувати графік та визначити властивості бінарного відношення:

а) $\alpha=\{<x,y>: x \in R \wedge y \in R \wedge (|x|+|y|=1)\}$

б) $\alpha=\{<x,y>: x \in R \wedge y \in R \wedge |x|=|y|\}$

2. Навести приклади бінарних відношень, які найбільш часто зустрічаються в шкільному курсі математики визначити їх властивості.

3. Чи можна стверджувати, що фактор-множина $A\backslash\alpha$ це розбиття множини A на різні класи еквівалентності?

4. Скільки всіх бінарних відношень можна утворити на множині, яка містить n елементів?

5. Яке бінарне відношення називається бінарною композицією двох бінарних відношень?

6. Яка множина називається впорядкованою множиною?

7. Яка множина називається частково впорядкованою множиною?

Лекція 2. Натуральні числа (аксіоми Пеано). Принцип математичної індукції

У 1891 році італійський математик Пеано запропонував таку акісоматичну побудову теорії модульних чисел.

Означення. Непорожня множина N, в якій для деяких елементів a і b існує відношення порядку "b слідує безпосередньо з a" і яке задовільняє такі аксіоми:

1. існує елемент e (одиниця), який не слідує безпосередньо за жодним іншим елементом;

2. для кожного елемента a існує і при тому лише один елемент - a', який слідує безпосередньо за a;

3. будь-який елемент, крім e, безпосередньо слідує за одним і тільки одним елементом;

4. якщо множина N має такі властивості:

а) $e \in N$;

б) якщо $a \in N$, то й $a' \in N$, то вона містить усі свої елементи, називається множиною натуральних чисел, а самі елементи множини N називаються натуральними числами. Очевидно, що множина чисел $1, 2, 3, \ldots$, які ми інтуїтивно засвоїмо в школі, задовольняють вимогам аксіоми Пеано.

Особлива роль належить четвертій аксіомі, бо вона є формально-логічною основою для доведення методом математичної індукції. На практиці аксіому 4 (її називають ще аксіомою індукції) використовують у формі принципу повної математичної індукції.

Теорема 1. Якщо твердження T, що містить натуральне число n, істине при $n=1$ і із істинності T при n випливає його істинність при $n+1$, то воно істинне для всіх натуральних чисел.

Доведення. Позначимо через N множину натуральних чисел, для яких твердження T істинне. Тоді $1 \in N$, бо для $n=1$ твердження T доведено. Нехай $n \in N$, тобто твердження T істинне для n. Тоді $n' \in N$, бо за теоремою, якщо T

істинне для n, то воно буде істинне і для n'. Згідно з аксіомою 4 множина N збігається з множиною всіх натуральних чисел, тобто T істинне для всіх натуральних чисел.

В багатьох випадках використовують інші форми принципу повної математичної індукції.

Теорема 2. Якщо про деяке твердження T відомо, що воно істинне для деякого натурального числа n і з припущенням, що T істинне для натурального числа $m \geq n$ випливає, що воно істинне для m', тоді T істинне для всіх натуральних чисел $m \geq n$.

Теорема 3. Якщо про деяке твердження відомо, що воно істинне при $n=1$ і з припущення, що T істинне для всіх натуральних менших $n(n>1)$ випливає, що воно істинне для n, то T істинне для всіх натуральних чисел.

Теорема 4. Якщо твердження T істинне при $к>1$ і з того, що воно істинне для всіх $к \leq m < n$ випливає, що воно істинне для n, то твердження T істинне для будь-якого числа $a \geq к$.

Вправи

1. Довести методом математичної індукції формулу Муавра.
2. Знайти суму $s=1^2+2^2+\ldots+n^2$
3. Довести, що $\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\frac{1}{7\cdot 10}+\ldots+\frac{1}{(3n-2)(3n+1)}=\frac{n}{3n+1}$

Лекція 3. Групи. Приклади груп. Основні властивості груп

<u>Означення 1</u>. Бінарної операцією на множині A називається відповідність, яка кожній впорядкованій парі елементів $a,b \in A$ співставляє лише один елемент c цієї ж множини A.

Бінарну операцію будемо позначати $c=a*b$. Як правило в математиці бінарні операції називають додаванням та множенням.

<u>Означення 2.</u> Множина G, в якій введена одна бінарна операція, відносно якої виконується три вимоги:

1. $(\underset{G}{\forall}\, a, b, c)((a*b)*c=a*(b*c));$

2. $(\underset{G}{\exists} e)(\underset{G}{\forall}\, a)(a*e=a)$ (елемент e називається правим нейтральним елементом);

3. $(\underset{G}{\forall}\, a)(\underset{G}{\exists} a^{-1})(a*a^{-1}=e)$ (елемент a^{-1} називається правим оберненим елементом).

називається групою.

Приклади:

1. Множина неособливих матриць n-го порядку є групою відносно операції множення матриць.

2. Множина парних чисел відносно операції додавання.

3. Множина цілих чисел відносно операції додавання.

Доведення проводяться безпосередньо перевіркою вимог групи.

Якщо бінарну операцію називають додаванням, то елемент e називають нулем і позначають θ, а елемент a^{-1} називають протилежним і позначають $-a$, а саму групу адитивною.

Якщо бінарну операцію називають множенням, то елемент e називають одиничним, а елемент a^{-1} називають оберненим до a, а саму групу – мультиплікативною.

Кількість елементів скінченої групи називають порядком групи. Якщо бінарна операція є комутативною, то групу називають комутативною або абелевою.

З означення групи випливають такі основні властивості.

<u>Властивість 1.</u> Кожний правий обернений елемент є одночасно і лівим оберненим елементом.

Доведення. Нехай a^{-1} є правим оберненим елементом, тобто $a*a^{-1}=e$. Виконаємо бінарну операцію зліва з елементом лівої та правої частини. Одержимо $a^{-1}*(a*a^{-1})=a^{-1}*e$ або $a^{-1}*(a*a^{-1})=a^{-1}$. Позначимо правий елемент до елемента a^{-1} через b. Виконаємо бінарну операцію справа з елементом b в останній рівності. Одержимо $(a^{-1}*(a*a^{-1}))*b= a^{-1}*b$ або $(a^{-1}*a)*(a^{-1}*b)=e$. Звідси слідує $a^{-1}*a=e$.

<u>Властивість 2.</u> Правий нейтральний елемент групи є одночасно лівим нейтральним елементів.

Доведення. Задано, що $a*a^{-1}=e$. Виконаємо бінарну операцію з елементом a справа. Одержимо $(a*a^{-1})*a=e*a$. Згідно властивості 1 маємо $a*(a^{-1}*a)=e*a$ або $a*e=e*a$.

<u>Властивість 3.</u> Нейтральний елемент в групі єдиний.

Доведення. Припустимо від супротивного, що в групі є два різні нейтральні елементи e_1 і e_2.

Тоді $\left.\begin{array}{l} e_1 * e_2 = e_1 \\ e_1 * e_2 = e_2 \end{array}\right| \Rightarrow e_1 = e_2.$

Що і треба було довести.

Аналогічно доводяться:

<u>Властивість 4.</u> $(\forall_G\, a,b)\ (\exists\, !x)(a*x=b)$

<u>Властивість 5.</u> $(\forall_G\, a,b)\ ((a*b)^{-1}=b^{-1}*a^{-1})$

<u>Властивість 6.</u> Кожний елемент a має єдиний обернений елемент a^{-1}.

Лекція 4. Підгрупи. Означення та критерій. Ізоморфізми та гомоморфізми груп. Основні властивості ізоморфізму

<u>Означення 1.</u> Підмножина *H* групи *G* називається підгрупою цієї групи, якщо вона сама є групою відносно бінарної операції групи *G*.

Кожна група має такі очевидні підгрупи: саму групу і підгрупу, яка складається лише з одного нейтрального елемента. Крім того група *G* може мати і інші підгрупи.

Приклади:

1. Підгрупами адитивної групи цілих чисел *Z* будуть множини Z_p цілих чисел, які кратні натуральним числам *p*.

2. Підгрупами мультиплікативної групи комплексних чисел $\{1, -1, i, -i\}$ будуть підмножини $\{1\}, \{1,-1\}, \{1,-1,i,-i\}$.

3. Множина всіх парних підстановок *n*-го степеня є підгрупою симетричної групи *n*-го степеня.

4. В мультиплікативній групі неособливих матриць *n*-го порядку підмножина матриць, визначники яких дорівнюють *1*, утворює підгрупу.

Для доведення того, що підмножини в прикладах 1-4 є підгрупами потрібно довести: 1) чи будуть бінарні операції груп бінарними операціями і підмножинах; 2) чи містять підмножини разом з будь-яким елементом а і його обернений елемент a^{-1}. (Розв'язання прикладів 1-4 рекомендуємо провести самостійно).

Теорема. Для того, щоб підмножина H групи G була підгрупою, необхідно і достатньо, щоб виконувалася умова

$$(\underset{H}{\forall} a,b)\ (a*b^{-1} \in H) \qquad (1)$$

Доведення. Необхідність. Так як *H* є підгрупою, то разом з будь-якими своїми елементами *a, b* вона містить і елемент b^{-1}, а значить і $a*b^{-1} \in H$.

Достатність. Так як H є підмножиною G, то асоціативність бінарної операції очевидна. Покажемо, що нейтральний елемент групи G належить H. Нехай a – будь-який елемент H. Тоді згідно умови (1) $e=a*a^{-1} \in H$.

Якщо $a \in H$, то використовуючи умову (1) до елементів e і a, маємо $a^{-1}=e*a^{-1} \in H$. Всі вимоги групи справджуються.

Потрібно ще довести, що бінарна операція групи G буде бінарною і в H. Нехай $a, b \in H$. Тоді і $b^{-1} \in H$ і згідно умови (1) $a*(b^{-1}) \in H$, або $a*b \in H$. Теорему доведено.

<u>Означення 2.</u> Групи G_1 і G_2 називаються ізоморфними, якщо між їхніми елементами можна встановити взаємно-однозначну відповідність таку, що якщо $x_1, y_1 \in G_1$ та $x_2, y_2 \in G_2$ і $x_1 \Leftrightarrow x_2, y_1 \Leftrightarrow y_2, x_1*y_1 \Leftrightarrow x_2*y_2$

Приклади:

1. Адитивна група G_1 цілих чисел ізоморфна адитивній групі перших чисел. Справді, якщо кожному цілому числу n поставити у відповідність парне число $2n$, то дістанемо ізоморфне відображення групи G_1 на G_2.

2. Мультиплікативна група G_1 додатних дійсних чисел ізоморфна адитивній групі G_2 всіх дійсних чисел.

Справді, якщо поставити у відповідність кожному додатному дійсному числу a дійсне число $lg\ a$, то отримаємо взаємно-однозначне відображення G_1 на G_2, яке буде ізоморфне, так як $lg\ a \cdot b = lga + lgb$.

Взаємно-однозначна відповідність називається при цьому ізоморфізмом. Якщо φ - ізоморфізм, то $\varphi(a*b)=\varphi(a)*\varphi(b)$.

<u>Означення 3.</u> Групи G_1 і G_2 називається гоморфними, якщо між їхніми елементами можна вставати відповідність (не вимагається взаємна однозначність) таку, що якщо $x_1, y_1 \in G_1$ та $x_2, y_2 \in G_2$ і $x_1 \Leftrightarrow x_2, y_1 \Leftrightarrow y_2$, то $x_1*y_1 \Leftrightarrow x_2*y_2$.

Відповідність при цьому називається гомоморфізмом.

Приклади:

1. Мультиплікативна група G_1 неособливих матриць n-го порядку гомоморфна мультиплікативній групі дійсних чисел відмінних від нуля. Справді, згідно теореми про визначник добутку матриць відповідність $\varphi : A \to det\ A$ буде гоморфізмом.

2. Мультиплікативна група підстановок 3-го степеня гомоморфна мультиплікативній групі $\{1, -1\}$.

Справді, співставивши парним підстановкам $+1$, а непарним -1, отримуємо гомоморфізм.

Для ізоморфізму та гоморфізму групи мають місце такі властивості.

<u>Властивість 1</u>. При ізоморфізмі (гомоморфізмі) φ образ нейтрального елемента $e \in G$ є нейтральним елементом $e_1 \in G_1$.

Доведення. Для кожного елемента a

$\varphi(a)= \varphi(a*e)= \varphi(a)* \varphi(e)$ або $(\varphi(a))^{-1}*\varphi(a)=((\varphi(a)^{-1}*\varphi(a) \varphi(e)$. Звідси слідує $\varphi(e)=e_1$.

<u>Властивість 2.</u> Для кожного елемента $a \in G$ образ $\varphi(a^{-1})$ оберненого елемента є оберненим елементом $(\varphi (a))^{-1}$ до образа $\varphi(a)$ елемента a.

Доведення. Позначимо через e_1 нейтральний елемент групи G_1. Тоді $e_1= \varphi(e)= \varphi(a*a^{-1})= \varphi(a)* \varphi(a^{-1})$. Звідси слідує, що $\varphi(a^{-1})=(\varphi(a))^{-1}$.

<u>Вправи.</u> Нехай a є будь-яким елементом групи G. Розглянемо множину всіх цілих степенів елемента a: $a^0=e, a^1, a^2, ..., a^{-1}, a^{-2}, ...$

Довести: 1. Множина всіх цілих степенів елемента а утворює підгрупу групи G, яка називається циклічною підгрупою.

<u>Означення 2.</u> Група G, яка співпадає з однією із своїх циклічних груп називається циклічною групою.

2. Довести, що кожна нескінченна циклічна група ізоморфна адитивній групі цілих чисел.

3. Довести, що циклічна група порядку n ізоморфна мультиплікативній групі коренів n-го степеня з одиниці.

Лекція 5. Кільце. Підкільце. Приклади кілець

Найпростіші властивості кілець. Ізоморфізми та гомоморфізми кілець.

<u>Означення 1.</u> Непорожня множина *K*, в якій визначено дві бінарні операції “додавання” і “множення” і виконуються вимоги:

1. $(\underset{K}{\forall}\, a, b, c)(a+b=b+a)$
2. $(\underset{K}{\forall}\, a, b, c)((a+b)+c=a+(b+c))$
3. $(\exists\theta)(\underset{K}{\forall}\, a)(a+\theta=a)$, θ - нульовий елемент
4. $(\underset{K}{\forall}\, a)(\underset{K}{\exists}(-a))(a+(-a)=\theta$
5. $(\underset{K}{\forall}\, a, b, c)((a\cdot(b\cdot c=(a\cdot b)\cdot c)$
6. $(\underset{K}{\forall}\, a, b, c)(a\cdot(b+c)=a\cdot b+a\cdot c)$
7. $(\underset{K}{\forall}\, a, b, c)(a+b\cdot c=a\cdot c+b\cdot c)$

називається кільцем.

Очевидно, що відносно операції додавання кільце *K* є абелевою групою, а тому можна стверджувати, що кільце *K* це абелева група відносно додавання, яка відносно множення асоціативна і пов’язана дистрибутивними законами відносно додавання.

Якщо операція множення є комутативна, то кільце *K* називається комутативним.

Приклади:

1. Множина цілих чисел – комутативне кільце відносно арифметичних операцій додавання і множення.

2. Множина парних чисел – комутативне кільце відносно арифметичних операцій додавання і множення.

3. Множина раціональних чисел *Q* відносно арифметичних операцій додавання і множення є комутативним кільцем

4. Множина дійсних чисел R є комутативним кільцем відносно операцій додавання і множення .

5. Множина класів лишків за модулем $m>1$ є комутативним кільцем відносно бінарної операції додавання і множення класів лишків.

6. Некомутативним кільцем є кільце квадратних матриць n-го порядку відносно операцій додавання і множення матриць над полями Q, R, C.

<u>Означення 2.</u> Підмножина K_1 кільця к називається підкільцем кільця K, якщо K_1 є кільцем відносно операцій додавання і множення, які визначені в кільці K.

Приклади:

1. Кільце парних чисел є підкільцем кілець R, Q, C.

2. Кільце матриць n-го порядку над полем Q є підкільцем кілець матриць n-го порядку над полями Q та C.

Теорема. Непорожня підмножина K_1 кільця K буде підкільцем тоді і тільки тоді, коли $a+b$, $a-b$, $a\cdot b$ будь-яких двох елементів a і b підмножини K_1 належали до K_1.

<u>Означення 2.</u> Елемент e_1 кільця K називається правим одиничним елементом, якщо $(\underset{K}{\forall} a)(a\cdot e_1=a)$

<u>Означення 3.</u> Елемент e_2 кільця K називається лівим одиничним елементом, якщо $(\underset{K}{\forall} a)(e_2\cdot a=a)$

Приклади:

1. Кільце парних чисел немає ні лівого ні правого одиничного елемента.

2. В кільці матриць другого порядку виду $\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}$ і $a,b\in R$ відносно операцій множення та додавання матриць є безліч лівих одиничних елементів. Справді, кожна матриця $\begin{pmatrix} 0 & 0 \\ m & 1 \end{pmatrix}$ для кожного $m\in R$ є лівим

одиничним елементом. $\begin{pmatrix} 0 & 0 \\ m & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}$, але ці матриці не будуть правими одиничними елементами, бо $\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}\begin{pmatrix} 0 & 0 \\ m & 1 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ b_m & b \end{pmatrix}$.

Якщо кільце K має і лівий одиничний елемент e_1 і правий одиничний елемент e_2, то вони співпадають. Справді, якщо e_1 вважають лівим одиничним елементом, то $e_1 \cdot e_2 = e_2$. Аналогічно, якщо e_2 вважають правим одиничним елементом, то $e_1 \cdot e_2 = e_1$.

З цих двох рівностей випливає, що $e_1 = e_2$.

<u>Означення 3.</u> Елемент кільця K називається одиничним елементом, якщо $(\forall_K a)(a \cdot e = e \cdot a = a)$.

<u>Означення 4.</u> Ненульове кільце, яке містить одиничний елемент e, називається кільцем з одиницею.

Прикладами кілець з одиницею є кільця Q, R, C. Кільцями з одиницею будуть кільце матриць n-го порядку над полями Q, R, C. В цих кільцях одиничним елементом буде одинична матриця.

<u>Означення 5.</u> Елементи a і b кільця K називаються дільниками нуля, якщо $a \neq 0$ і $b \neq 0$, але $a \cdot b = 0$. a називають лівим дільником нуля, b називають правим дільником нуля.

Приклади :

1. В кільці квадратних матриць другого порядку над полями R, Q, C матриці $\begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix}$ та $\begin{pmatrix} 0 & 0 \\ 0 & n \end{pmatrix}$ будуть дільниками нуля, бо $\begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & n \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

2. В кільці неперервних функцій проміжку $[-1, 1]$ відносно початкового додавання і множення дільниками нуля будуть функції

$$f_1(x)=\begin{cases} 0, & -1 \le x \le 0 \\ x, & 0 < x \le 1 \end{cases} \text{ та } f_2(x)=\begin{cases} -x, & -1 \le x \le 0 \\ 0, & 0 < x \le 1 \end{cases} \text{ бо } f_1(x) \cdot f_2(x) = 0.$$

<u>Означення 6.</u> Комутативне кільце, в якому немає дільників нуля, називають областю цілісності.

З означення кільця випливають такі основні властивості

1. $(\underset{K}{\forall} a, b)(a+b=a \Rightarrow b=0)$

2. $(\underset{K}{\forall} a, b)(a+b=0 \Rightarrow b=-a)$

3. $(\underset{K}{\forall} a)(-(-a)=a)$

4. $(\underset{K}{\forall} a)(0\cdot a=a\cdot 0=0)$

5. $(\underset{K}{\forall} a, b)((-a)\cdot b=a\cdot(-b)=-(a\cdot b))$

6. $(\underset{K}{\forall} a, b)((-a)\cdot(-b)=a\cdot b)$

7. $(\underset{K}{\forall} a, b,c)(a\cdot(b-c)=a\cdot b-a\cdot c)$

8. $(\underset{K}{\forall} a, b,c)((a-b)\cdot c=a\cdot c-b\cdot c)$

Доведемо, наприклад, властивості 1,8.

Якщо $a+b=a$, то $b=0+b=(-a+a)+b=-a+(a+b)=-a+0=-a$.

З (5) і дистрибутивності множення відносно додавання слідує, що $(a-b)\cdot c=(a+(-b)\cdot c=a\cdot c+(-b)\cdot c=a\cdot c+(-b\cdot c)=a\cdot c-b\cdot c$.

<u>Означення 7.</u> Відображення $\varphi: K_1 \to K_2$ кільця K_1 в кільце K_2 називають гомоморфним відображенням або гомоморфізмом K_1 в K_2, якщо:

1. $(\underset{K_1}{\forall} a, b)(\varphi(a+b)= \varphi(a)+ \varphi(b))$

2. $(\underset{K_1}{\forall} a, b)(\varphi(a\cdot b)= \varphi(a)\cdot\varphi(b))$

Приклади:

1. Безпосередньою перевіркою вимог 1, 2 переконуємося, що кільце C комплексних чисел гомоморфне кільцю матриць другого порядку над полем C. Гомоморфізм задається, наприклад, так $(\underset{C}{\forall}(a+bi))(\varphi(a+bi)=\begin{pmatrix} a & b \\ -b & a \end{pmatrix})$

2. Кільце матриць другого порядку $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ над полем дійсних чисел гомоморфне кільцю дійсних чисел R.

Безпосередньою перевіркою вимог *1*, *2* переконуємося, що $\underset{R}{\forall}(a,b)(\varphi\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} = a + b\sqrt{2}$ є гоморфізмом.

Основними властивостями гомоморфізму є:

<u>Властивість 1.</u> Якщо φ є гомоморфізмом кільця K_1 в кільце K_2, то $\varphi(0)=0_1$

<u>Властивість 2.</u> Якщо φ є гомоморфізмом кільця K_1 в кільце K_2, то $(\underset{K_1}{\forall} a)\ (\varphi(-a)= -\varphi(a))$.

<u>Означення 8.</u> Взаємно однозначне відображення φ кільця K_1 на кільце K_2 при якому: $(\underset{K_1}{\forall} a, b)(\varphi(a+b)= \varphi(a)+ \varphi(b))$, $(\underset{K_1}{\forall} a, b)(\varphi(a\cdot b)= \varphi(a)\cdot\varphi(b))$ називається ізоморфізмом кілець K_1 та K_2. Самі кільця K_1 та K_2 називаються при цьому ізоморфними.

<u>Означення 9.</u> Скалярною матрицею над полем *П* називається матриця *n*-го порядку елементами головної діагоналі якої є одне і те саме число *m*, а решта елементів дорівнюють нулеві.

Безпосередньою перевіркою переконуємося, що кільце скалярних матриць *n*-го порядку ізоморфне кільце дійсних чисел *R*. Ізоморфізмом при цьому буде

$$\varphi: \begin{pmatrix} n & 0 & \dots & 0 \\ 0 & n & \dots & 0 \\ & & \dots & \\ 0 & 0 & \dots & n \end{pmatrix} \to n$$

Як і при гоморфізмі кілець доводяться такі основні властивості ізоморфізму.

<u>Властивість 1.</u> Якщо φ ізоморфізм кільця K_1 на кільце K_2, то $\varphi(0)=0_1$

<u>Властивість 2.</u> Якщо φ ізоморфізм кільця K_1 на кільце K_2, то $(\underset{K_1}{\forall} a)\ (\varphi(-a)= -\varphi(a))$.

Лекція 6. Поле. Підполе. Приклади. Основні властивості полів. Поле дійсних чисел

<u>Означення 1.</u> Множина P, яка містить принаймні два різних елементи, в якій введені дві бінарні операції “додавання” і “множення” і виконуються вимоги:

1. $(\underset{P}{\forall}\, a, b)(a+b=b+a)$
2. $(\underset{P}{\forall}\, a, b, c)((a+b)+c=a+(b+c))$
3. $(\underset{P}{\forall}\, a, b)\ (\underset{P}{\exists}\, x)(a+x=b)$
4. $(\underset{P}{\forall}\, a, b)(a\cdot b=b\cdot a)$
5. $(\underset{P}{\forall}\, a, b, c)((a\cdot b)\cdot c=(a\cdot(b\cdot c))$
6. $(\underset{P}{\forall}\, a, b, c)(a\cdot(b+c)=a\cdot b+a\cdot c)$
7. $(\underset{P}{\forall}\, a\#\theta)(\underset{P}{\forall}\, b)(\underset{P}{\exists} x)\ (a\cdot x=b)$

називається полем.

<u>Означення 2.</u> Підмножина P_1 поля P називається підполем поля P, якщо вона сама є полем відносно тих самих операцій “додавання” і “множення” поля P.

Приклади:

1. Множини Q, R, C відносно операцій додавання і множення утворюють поля.

2. Множина чисел виду $a+b\sqrt{2}$, $a,b\in Q$ відносно операцій додавання і множення утворює поле.

3. Поле Q, R є підполем поля C.

4. Поле Q є підполем поля R.

5. Множина матриць виду $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, $a,b\in Q$ відносно операції додавання і множення матриць утворює поле.

З означення поля випливають такі основні властивості:

1. У кожному полі існує і притому єдиний нульовий елемент.

Доведення. Нехай $a \in P$. Згідно вимоги 3 поля, рівняння $a+n=a$ має розв'язок n. Якщо b – будь-який інший елемент поля P, то рівняння $a+n=b$ також має розв'язок m. Тоді $b+n=(a+m)+n=(m+a)+n=m+(a+n)=m+a=a+m=b$. Тобто, $b+n=n+b=b$.

Доведемо, що нульовий елемент єдиний методом від супротивного, використовуючи модифікацію

$A \Rightarrow B \equiv A \wedge \overline{B} \Rightarrow B$

Нехай θ_1 і θ_2 різні нульові елементи. Тоді $\theta_1 + \theta_2 = \theta_1$, якщо вважати θ_2 за нульовий елемент $\theta_1 + \theta_2 = \theta_2$, якщо вважати θ_1 за нульовий елемент. З цих двох співвідношень випливає, що $\theta_1 = \theta_2$.

Означення 3. Елемент е поля Р називається одиничний, якщо $(\forall_P a)(a \cdot e = e \cdot a = a)$.

2. У кожному полі існує і притому єдиний одиничний елемент. Доведення властивості 2 аналогічне доведенню властивості 1.

3. Кожний елемент $a \in P$ має і притому єдиний протилежний елемент – $-a$.

Доведення. Згідно з вимогою 3 поля P рівняння $a+x=\theta$ має розв'язок $x \in P$, який і буде протилежним елементом до a. Єдиність доведемо методом від супротивного, використовуючи ту ж саму модифікацію, що і у доведенні властивості 1. Нехай y, x різні протилежні елементи до елемента a. Тоді $x=x+\theta=x+(a+y)=(x+a)y=\theta+y=y$, що і треба було довести

4. Кожний елемент $a \neq \theta$ поля P має єдиний обернений елемент a. Доведення аналогічне доведенню властивості 3.

5. Поле P не має дільників нуля.

Доведення. Нехай $a \neq \theta$, але $a \cdot b = \theta$. Оскільки $a \neq \theta$, то існує єдиний обернений елемент a^{-1}. Помножимо рівність $a \cdot b = \theta$ на a^{-1}. Отримаємо $b = \theta$.

Тобто, якщо добуток елементів дорівнює нульовому елементу, то принаймні один з множників відмінний від θ.

Серед інших властивостей відмітимо:

6. Якщо $a+b=a+c$, то $b=c$

<u>Означення 4</u>. Різницею $b-a$ елементів b та a називається такий елемент $x \in P$, для якого виконується рівність $a+x=b$.

Таким чином, $a+(b-a)=(b-a)+b$. $a-a=0$, $0-a=-a$.

7. $(\forall_{P}\, a,b)(a-b=a+(-b))$

8. $(\forall_{P}\, a, b, c)((a-b)\cdot c=a\cdot c-b\cdot c)$

<u>Означення 5.</u> Множина $П$, яка містить принаймні два різних елементи, в якій визначена властивість елементів "бути додатними" (>0) і визанчені дві бінарні операції "додавання"$(+)$ та "множення" $(\cdot)$ і виконуються вимоги:

1. $((\forall_{П}\, a,b)(a+b=b+a)$

2. $(\forall_{П}\, a,b,c)((a+b)+c=a+(b+c))$

3. $(\forall_{П}\, a,b)(\exists x)(a+x=b)$

4. $(\forall_{П}\, a,b)(a\cdot b=b\cdot a)$

5. $(\forall_{П}\, a,b,c)((a\cdot b)\cdot c=a\cdot(b\cdot c))$

6. $(\forall_{П}\, a,b,c)((a\cdot(b+c)=a\cdot b+a\cdot c)$

7. $(\forall_{П}\, a\neq\theta)(\forall b)(\exists x)(a\cdot x=b)$

8. Для кожного елемента $a \in П$ виконується одне і тільки одне з співвідношень: $a=\theta \vee a>0 \vee -a>0$

9. $(\forall_{П}\, a,b)(a>\theta \wedge b>\theta \Rightarrow a+b>\theta \wedge a\cdot b>\theta)$

Вважатимемо, що $a>b \Leftrightarrow a-b>\theta$

10. Аксіома Архімеда $(\forall_{П}\, a)(\forall_{П}\, b>\theta)(\exists_{N}\, n)(n\cdot b>a)$

11. Аксіома повноти. Будь-яка фундаментальна послідовність $\{a_n\}$ елементів з Π має границю в Π називається полем дійсних чисел, а самі елементи поля Π – дійсними числами.

Нагадаємо, що:

<u>Означення 6.</u> Послідовність $\{a_n\}$ елементів поля Π називається фундаментальною, якщо для будь-якого елемента $\varepsilon>\theta$ із Π існує таке натуральне число n_a (залежне від a), що $|a_p - a_q| < \varepsilon$ для всіх p, q більших від n_a.

<u>Означення 7.</u> Поле називається розташованим, якщо виконуються аксіоми 8, 9.

<u>Означення 8.</u> Розташоване поле в якому виконується аксіома Архімеда називається архімедовим розташованим полем.

<u>Означення 9.</u> Розташоване поле називається повним, якщо кожна фундаментальна послідовність є збіжною в цьому полі.

Якщо врахувати наведені вище означення, то означити поле дійсних чисел можна так.

<u>Означення 10.</u> Повне розташоване архімедове поле, яке містить у собі підполе раціональних чисел Q називається полем дійсних чисел.

Лекція 7. Поле комплексних чисел. Алгебраїчна та тригонометрична форма

Вивчаючи шкільних курс математики, учні поступово ознайомлюються з натуральними, цілими, раціональними, ірраціональними, дійсними числами.

Відомо, що дійсних чисел недостатньо для того, щоб розв'язувати рівняння, дискримінанти яких від'ємні. Отже, в шкільному курсі математики виникла необхідність розширення дійсних чисел таких, щоб в розширеній системі можна було розв'язувати всі квадратні рівняння. Множина дійсних чисел геометрично вичерпується точками числової прямої, а, значить, природно шукати розширення дійсних чисел на площині. Таким чином, ми визначимо множину чисел, які зображуються точками площини.

Нехай на площині вибрана прямокутна декартова система координат. Точки площини будемо позначати малими грецькими буквами.

<u>Означення 1.</u> Впорядкована пара чисел $a,\ b$ називається комплекним числом і позначається $\alpha=\langle a,b\rangle$.

<u>Означення 2.</u> Два комплексні числа $\alpha=\langle a,b\rangle$, $\beta=\langle c,d\rangle$ називаються рівними, якщо $a=c\wedge b=d$ і записуємо $\alpha=\beta$.

<u>Означення 3.</u> "Сумою" $\alpha+\beta$ двох комплексних чисел $\alpha=\langle a,b\rangle$, $\beta=\langle c,d\rangle$ називається комплексне число $\gamma=\langle k,m\rangle$, для якого $k=a+c \wedge m=b+d$.

<u>Означення 4.</u> "Добутком" $\alpha\cdot\beta$ двох комплексних чисел α та β називається таке комплексне число $\delta=\langle r,n\rangle$, для якого $r=ac-bd \wedge n=ad+bc/$

Таким чином $\gamma=\alpha+\beta=\langle a+c,b+d\rangle$, $\delta=\alpha\cdot\beta=\langle ac-bd,ad-bc\rangle$. Очевидно, що ці операції є бінарні. Доведемо, що множина всіх комплексних чисел, відносно операцій "+" та "·" утворює поле. Для цього потрібно перевірити виконання вимог (1-7) поля. Перевірка істинності вимог 1, 2, 3, 4, 5, 6 проводиться безпосереднім обчисленням лівої та правої частини та їх порівняння. Доведемо, наприклад, властивість 2. $(\forall\ \alpha,\ \beta,\ \gamma)((\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma))$

Обчислюємо ліву частину. $(\alpha\cdot\beta)\cdot\gamma=(<a,b>\ <c,d>)\ <k,m>=<ac-bd,\ ad+bc>\ <k,m>=<(ac-bd)k-(ad+bc)m,(ac-bd)m+(ad+bc)k>=<ack-bdk-adm-bcm,\ acm-bdm+adk+bck>$

Обчислюємо праву частину $\alpha\cdot(\beta\cdot\gamma)=<a,b>\ (<c,d>\ <k,m>)=<a,b>\cdot<ck-dm,\ cm+dk>=<a(ck-dm)-b(cm-dk),\ a(cm+dk)+b(ck-dm)>=<ack-adm-bcm-bdk,\ acm+adk+bck-bdm>$ Порівнюючи одержані результати переконуємося, що $(\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma)$

Доведемо вимогу 3. Покажемо, що для будь-яких комплексних чисел α, β рівняння $\alpha+\chi=\beta$ має розв'язок. Справді $<a,b>+<x,y>=<c,d>$. Звідси $x=c-a$, $y=d-b$. Таким чином $\chi=<c-a,\ d-b>$ і буде розв'язком рівняння $\alpha+\chi=\beta$.

Доведемо вимогу 7. Очевидно, що $\theta=<0,0>$. Покажемо, що рівняння $\alpha\cdot\chi=\beta$, $\alpha\neq\theta$ має розв'язок. Справді $<a,b><x,y>=<c,d>$. Звідси отримуємо

$$\begin{cases} ax-by=c \\ bx+ay=d \end{cases}$$

Розв'язуючи цю систему рівнянь маємо $x=\dfrac{ac+bd}{a^2+b^2}$, $y=\dfrac{ad-bc}{a^2+b^2}$.

Побудоване поле комплексних чисел позначимо C.

З доведення вимог 3, 7 поля C випливає, що різницею $\alpha-\beta$ двох комплексних чисел буде $<a-c,b-d>$, часткою буде $\dfrac{\beta}{\alpha}=<\dfrac{ac+bd}{a^2+b^2},\ \dfrac{ad-bc}{a^2+b^2}>$. Якщо $\alpha=\beta$, то ми отримаємо, що одиничним елементом буде $<1,\ 0>$. Якщо $\beta=<1,\ 0>$, то $\alpha^{-1}=\dfrac{a}{a^2+b^2},\ \dfrac{-b}{a^2+b^2}$.

Побудоване поле комплексних чисел є розширенням поля дійсних чисел. Справді, розглянемо точки, які належать осі $0x$, тобто точки виду $<a,0>$. Якщо комплексному числу $<a,0>$ співставити дійсне число а, то ми отримаємо взаємно однозначну відповідність між точками осі $0x$ і множиною дійсних чисел. Так як $<a,0>+<c,0>=<a+c,0>$. $<a,0>\cdot<c,0>=<a\cdot c,0>$, то комплексні числа виду $<a,0>$ додаються і перемножуються як дійсні числа, а тому вважатимемо, що комплексні числа $<a,0>$ ототожнюються з дійсними

числами а, зокрема $<1,0>=1$ і $<0,0>=0$. Покажемо, що серед комплексних чисел є таке число квадрат якого дорівнює -1. Обчислимо квадрат числа $<1,0>$. $<0,1>\cdot<0,1>=<-1,0>=-1$.

Точка $<0,1>$ лежить на осі ординат. Цю точку прийнято позначати буквою i, так що $i^2=-1$. Комплексне число $<a,b>$ можна записати ще так

$$<a,b>=<a,0>+<0,b>=<a,0>+<b,0><0,1>=a+b\cdot i$$

<u>Означення 5</u>. Представлення комплексного числа $<a,b>$ у виді $a+bi$ називається алгебраїчною формою.

Комплексне число і називають уявною одиницею, числа виду $b\cdot i$ – уявними числами. В записі комплексного числа α у виді $a+bi$ числа a називають дійсною частиною числа α, а bi – уявною частиною. Площину, точками якої є комплексні числа, називають комплексною площиною. Вісь абсцис називають дійсною віссю, а вісь y – уявною віссю.

Дії над комплексними числами в алгебраїчній формі здійснюються так:

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$

$$(a+bi)-(c+di)=(a-c)+(b-d)i$$

Тобто, щоб додати (відняти комплексні числа потрібно додати(відняти) окремо їх дійсні і уявні частини.

$$(a+bi)(c+di)=(ac-bd)+(ad+bc)i$$

Тобто, множення комплексних чисел здіснюється за правилами множення двочленів.

$$\frac{c+di}{a+bi}=\frac{(a-bi)\cdot(c+di)}{(a-bi)\cdot(a+bi)}=\frac{ac+bd}{a^2+b^2}+\frac{ad-bc}{a^2+b^2}\cdot i$$

Правило ділення комплексних чисел громіздке, а тому його не запам’ятовують. Потрібно лише пам’ятати, що при діленні комплексних чисел в алгебраїчній формі потрібно чисельник і знаменник дробу помножити на число, яке відрізняється від знаменника лише знаком уявної частини (це число називається спряженим).

Запис комплексного числа α в алгебраїчній формі $a+bi$ використовує декартові координати точки, які відповідають даному числу. Положення

точки на площині повністю визначається заданням її полярних координат: віддалі r від початку координат до точки α і кута φ між додатнім напрямом осі абсцис і напрямом від початку координат на цю точку.

Число r – завжди невід'ємне, і дорівнює нулеві лише для точки 0; його називають модулем комплексного (для чисел осі $0x$ модуль комплексного числа співпадає з абсолютною величиною числа) і позначають $|\alpha|$.

Кут φ називають аргументом комплексного числа і позначають $arg\ \alpha$. Вважають, що $0 \le arg\ \alpha < 2\pi$ або $-\pi \le arg\ \alpha < \pi$.

Між декартовими і полярними координатами точки справедливі такі співвідношення

$$a = r\cos\varphi,\ b = r\sin\varphi \qquad (1)$$

Звідси

$$r = \sqrt{a^2 + b^2} \qquad (2)$$

Тоді $a+bi = r\cos\varphi + i\,r\sin\varphi = r(\cos\varphi + i\sin\varphi)$, тобто

$$a+bi = r(\cos\varphi + i\sin\varphi) \qquad (3)$$

Навпаки, нехай число $\alpha = a+bi$ допускається запис $\alpha = r_0(\cos\varphi_0 + i\sin\varphi_0)$, де r_0, φ_0 – деякі дійсні числа, при цьому $r \ge 0$. Тоді $r_0\cos\varphi_0 = a$, $r_0\sin\varphi_0 = b$. Звідки $r_0 = +\sqrt{a^2+b^2}$, тобто з (2) слідує, що $r_0 = |\alpha|$. Використовуючи (1) отримаємо: $\cos\varphi_0 = \cos\varphi$, тобто $arg\ \alpha = \varphi_0$. Таким чином кожне комплексне число однозначно записується в виді (3), де $r = |\alpha|_i$ і $\varphi = arg\ \alpha$.

Запис комплексного числа в виді (3) називається його тригонометричною формою.

Дії над комплексними числами в тригонометричній формі здійснюються так. Нехай $\alpha = r(\cos\varphi + i\sin\varphi)$, $\beta = \rho(\cos\theta + i\sin\theta)$. Перемножуємо їх $\alpha\cdot\beta = [\,r(\cos\varphi + i\sin\varphi)][\beta = \rho(\cos\theta + i\sin\theta)] = r\rho(\cos\varphi\cos\theta + i\cos\varphi\sin\theta + +i\sin\varphi\cos\theta + +I^2\sin\varphi\sin\theta) = r\rho(\cos(\varphi+\theta) + i\sin(\varphi+\theta))$.

Щоб помножити два комплексні числа в тригонометричній формі потрібно модулі перемножити і аргументи додати. Нехай $\beta \ne 0$, тоді

$$\frac{\alpha}{\beta}=\frac{r(\cos\varphi+i\sin\varphi)}{\rho(\cos\theta+i\sin\theta)}=\frac{[r(\cos\varphi+i\sin\varphi)][\rho(\cos\theta-i\sin\theta)]}{[\rho(\cos\theta+i\sin\theta)][\rho(\cos\theta-i\sin\theta)]}=$$

$$=\frac{r}{\rho}\frac{\cos\varphi\cos\theta-i\cos\varphi\sin\varphi+i\sin\varphi\cos\theta-i^2\sin\varphi\sin\theta}{\cos^2\theta+\sin^2\theta}=\frac{r}{\rho}(\cos(\varphi-\theta)+i\sin(\varphi-\theta))$$

Щоб поділити комплексні числа в тригонометричній формі потрібно їх модулі поділити, а аргументи відняти.

Вправи:

1. Знайти дійсну і уявну частини комплексних чисел:

   а) $\frac{(1+2i)^3-(1+3i)^3}{(3-i)^3+(1+5i)^2}$

   б) $(2-3i)^4+(2+3i)^4$

2. Розв’язати рівняння:

   $z^2+5z+5-3i=0$

3. Обчислити:

   а) $\frac{(1+i\sqrt{3})^{30}}{(1-i\sqrt{3})^{15}}$

   б) $\frac{1-i}{1+i}$

4. Довести властивості:

   а) $\overline{\alpha+\beta}=\overline{\alpha}+\overline{\beta}$

   б) $\overline{\alpha\cdot\beta}=\overline{\alpha}+\overline{\beta}$

   в) $\overline{\left(\frac{\alpha}{\beta}\right)}=\frac{\overline{\alpha}}{\overline{\beta}}$

Лекція 8. Системи лінійних рівнянь. Основні означення

Розв'язування систем лінійних рівнянь методом послідовного виключення невідомих.

<u>Означення 1.</u> Лінійною неоднорідною системою рівнянь, яка містить m рівнянь і n невідомих називається:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = b_1 \\ a_{21}x_2 + a_{22}x_2 + ... + a_{2n}x_n = b_2 \\ \qquad\qquad \cdots \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n = b_m \end{cases} \qquad (1)$$

Тут $x_1, x_2, \ldots, x_n$ – шукані невідомі; $a_{11}, a_{12}, \ldots, a_{mn}$ – коефіцієнти при невідомих; $b_1, b_2, \ldots, b_m$ – вільні члени. Вважаємо всі ці величини дійсними числами. Кількість рівнянь та кількість невідомих може бути різною. Якщо всі вільні члени дорівнюють нулеві, то система рівнянь називається однорідною лінійною системою рівнянь.

<u>Означення 2.</u> Вектор $\bar{a}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ називається розв'язком лінійної неоднорідної системи рівнянь (1), якщо при підстановці його компонент замість невідомих $x_1, x_2, \ldots, x_n$ кожне з рівнянь перетворюється в істинну числову рівність.

<u>Означення 3.</u> Система рівнянь (1) називається сумісною, якщо вона має хоч би один розв'язок.

<u>Означення 4.</u> Система рівнянь називається несумісною, якщо множина її розв'язків порожня.

Розв'язати систему рівнянь (1) означає або знайти всі її розв'язки або довести, що система (1) не має розв'язків.

Сумісна система рівнянь має або один розв'язок або безліч розв'язків.

В багатьох випадках систему (1) доцільно записувати у векторно-скалярній, векторній і матричній формі.

Якщо розглядати ліву частину кожного рівняння системи (1) як скалярний добуток відповідного вектора-рядка на вектор невідомих $\bar{x}=(x_1,x_2,\ldots,x_n)$, то систему (1) можна записати так:

$$(\overline{a_i}\,,\ \bar{x})=\bar{b}_i\,,\ i=\overline{1,m} \qquad (2)$$

це векторно-скалярний запис системи рівнянь.

Якщо позначити через $\overline{p_1}\,,\ \overline{p_2}\,,\ \ldots\,,\ \overline{p_n}$ вектори стовпці при відповідних невідомих, то систему рівнянь (1) можна записати так:

$$x_1\overline{p_1}+x_2\overline{p_2}+\ldots+x_n\overline{p_n}=\bar{b} \qquad (3)$$

Це векторний запис системи рівнянь.

Якщо A – основна матриця системи, X – матриця-стовпець невідомих, B – матриця-стовпець вільних членів, то систему рівнянь (1) можна записати так:

$$AX=B \qquad (4)$$

це матрична форма запису системи рівнянь (1).

<u>Означення 4.</u> Дві системи лінійних рівнянь називаються еквівалентними (рівносильними), якщо кожний розв’язок однієї системи рівнянь є розв’язком другої системи рівнянь і навпаки.

<u>Означення 5</u>. Елементарними перетвореннями системи рівнянь називаються на ступні перетворення:

1. перестановка місцями будь-яких двох рівнянь системи;
2. множення будь-якого рівняння на відмінне від нуля число;
3. додавання до обидвох частин одного рівняння відповідних частин другого рівняння, які помножені на відмінне від нуля число.

Очевидно, що елементарні перетворення переводять дану систему рівнянь в еквівалентну систему.

Розглянемо метод Гауса. Нехай в першому рівнянні системи (1) коефіцієнт $a_{11}\neq 0$ (якщо це не так, то поміняємо місцями доданки лівої частини і проведемо аналогічні міркування). Перетворимо систему рівнянь (1), виключивши змінну x_1 з усіх рівнянь, крім першого. Для цього

помножимо обидві частини першого рівняння на $-\frac{a_{21}}{a_{11}}$ і до другого рівняння додаємо перетворене перше, відтак перше рівняння помножимо на $-\frac{a_{31}}{a_{11}}$ і до третього рівняння додамо перетворене перше і так далі, нарешті, помножимо перше рівняння на $-\frac{a_{m1}}{a_{11}}$ і до *m*-го рівняння додамо перетворене перше рівняння. В результаті отримаємо

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = b_1 \\ \qquad a'_{22}x_2 + ... + a'_{2n}x_n = b'_2 \\ \qquad a'_{32}x_2 + ... + a'_{3n}x_n = b'_3 \\ \qquad\quad . \; . \; . \\ \qquad a'_{m2}x_2 + ... + a'_{mn}x_n = b'_m \end{cases} \tag{5}$$

Тут коефіцієнти a'_{ij} та вільні члени b'_i вирази коефіцієнтів та вільних членів, які отримані після виконаних перетворень. Система рівнянь (5) очевидно буде еквівалентною системі (1). Перше рівняння системи залишаємо без змін. Розглянемо друге, третє і т. д. *m*-те рівняння. Якщо серед цих рівнянь є такі, що всі коефіцієнти лівої частини та відповідний вільний член дорівнює нулеві, тобто виду $0 \cdot x_2 + 0 \cdot x_3 + ... + 0 \cdot x_n = 0$, то ми ці рівняння виключаємо з розгляду. Якщо серед рівнянь є такі, що всі коефіцієнти лівої частини *0*, а відповідний вільний член правої частини відмінний від нуля, тобто $0 \cdot x_2 + 0 \cdot x_3 + ... + 0 \cdot x_n = b,\ b \neq 0$, то тим самим ми вже довели, що система рівнянь несумісна. Таким чином, вважаємо, що серед коефіцієнтів a'_{ij} є відмінні від нуля. Нехай, наприклад $a'_{22} \neq 0$. Аналогічно до описаних вище перетворень, домножаємо друге рівняння відповідно на $-\frac{a'_{31}}{a'_{11}}$, … , $-\frac{a'_{m2}}{a'_{22}}$ і перетворене друге рівняння додаємо до третього і т. д. m-го рівняння. Отримаємо:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + ... + a_{1n}x_n = b_1 \\ a'_{22}x_2 + a'_{23}x_3 + ... + a'_{2n}x_n = b'_2 \\ a''_{33}x_2 + ... + a''_{3n}x_n = b''_3 \\ \cdot\ \cdot\ \cdot \\ a''_{m3}x_3 + ... + a''_{mn}x_n = b''_m \end{cases} \qquad (6)$$

Система рівнянь (6) еквівалентна до системи рівнянь (5), а значить і до системи рівнянь (1). Зауважимо, що кількість рівнянь могло зменшитися вже після першого кроку. Проводимо знову аналогічні міркування до проведених вище.

Коли ж закінчиться процес послідовного виключення змінних?

Якщо ми отримаємо систему рівнянь коефіцієнти лівої частини нулі, а вільний член є відмінний від нуля, то наша система рівнянь (1) є несумісною.

В усіх інших випадках ми отримаємо систему рівнянь виду:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1k-1}x_{k-1} + a_{1k}x_k + ... + a_{1n}x_n = b_1 \\ a'_{22}x_2 + ... + a'_{2k-1}x_{k-1} + a'_{2k}x_k + .. + a'_{2n}x_n = b'_2 \\ \cdot\ \cdot\ \cdot \\ a^{(k-2)}_{k-1k-1}x_{k-1} + a^{(k-2)}_{k-1k}x_k + ... + a^{(k-2)}_{k-1n}x_n = b^{(k-2)}_{k-1} \\ a^{(k-1)}_{kk}x_k + ... + a^{(k-1)}_{kn}x_n = b^{(k-1)}_k \end{cases} \qquad (7)$$

в якій $a_{11} \neq 0,\ a'_{22} \neq 0,\ \ldots,\ a^{(k-2)}_{k-1k-1} \neq 0,\ a^{(k-1)}_{kk} \neq 0;\ k \leq m,\ k \leq n.$

Система рівнянь (7) сумісна. Якщо $k=n$, то система (7) матиме вид

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = b_1 \\ a'_{22}x_2 + ... + a'_{2n}x_n = b'_2 \\ \cdot\ \cdot\ \cdot \\ a^{(n-1)}_{nn}x_n = b^{(n-1)}_n \end{cases} \qquad (8)$$

З останнього рівняння визначимо x_n. Підставивши його значення в передостаннє рівняння визначимо x_{n-1}. Продовжуючи цей процес ми отримаємо, що система рівнянь (8), а значить і система рівнянь (1) мають єдиний розв’язок.

Якщо $k<n$, то залишимо в кожному рівнянні системи (7) в лівій частині доданки першими k невідомими, а інші – перенесемо в праву частину. Зафіксуємо будь-яким способом невідомі $x_{k+1}, \ldots, x_n$ правої частини.

Отримуємо конкретні значення для $x_1, x_2, \ldots, x_k$. Так як фіксувати невідомі x_{k+1}, … , x_n можна безліччю способів, то в цьому випадку система рівнянь (7), а значить і (1) має безліч розв'язків.

Зауваження. Застосувавши метод Гаусса до однорідної системи рівнянь, отримуємо, що вона завжди сумісна, бо $\bar{\theta}(0, 0, \ldots, 0)$ є її розв'язком і має або безліч розв'язків, або лише нульовий розв'язок.

Вправи. Розв'язати систему рівнянь методом Гаусса:

а) $\begin{cases} x_1 + 2x_2 - 5x_3 = 0 \\ 2x_1 + 3x_2 - 2x_3 = 6 \\ 3x_1 + 2x_2 + x_3 = 8 \end{cases}$

б) $\begin{cases} x_1 + 3x_2 + x_3 + x_4 = 1 \\ 2x_1 + 4x_2 + 3x_3 - x_4 = 2 \\ 3x_1 + 2x_2 - 3x_3 + x_4 = 3 \end{cases}$

Лекція 9. Арифметичний *n*-вимірний векторний простір. Лінійна залежність і лінійна незалежність множини векторів. Ранг і базис скінченної множини векторів

<u>Означення 1</u>. Впорядкований набір n дійсних чисел називається *n*-вимірним вектором.

Символічно *n*- вимірний вектор з компонентами $a_1, a_2, \ldots, a_n$ записуватимемо так $\bar{a} = (a_1, a_2, \ldots, a_n)$.

<u>Означення 2.</u> Два *n*-вимірні вектори $\bar{a} = (a_1, a_2, \ldots, a_n)$ та $\bar{b} = (b_1, b_2, \ldots, b_n)$ називаються рівними, якщо рівні всі їх відповідні компоненти.

<u>Означення 3.</u> Сумою двох *n*-вимірних векторів $\bar{a} = (a_1, a_2, \ldots, a_n)$ та $\bar{b} = (b_1, b_2, \ldots, b_n)$ називається вектор $\bar{c} = (a_1+b_1, a_2+b_2, \ldots, a_n+b_n)$.

<u>Означення 4.</u> Під добутком дійсного числа λ на *n*-вимірний вектор $\bar{a} = (a_1, a_2, \ldots, a_n)$ розуміють вектор $\bar{a}\lambda = \lambda\bar{a}$ $(\lambda a_1, \lambda a_2, \ldots, \lambda a_n)$.

З наведених вище означень випливають такі основні властивості:

1. $(\forall \bar{a}, \bar{b})(\bar{a} + \bar{b} = \bar{b} + \bar{a})$;
2. $(\forall \bar{a}, \bar{b}, \bar{c})((\bar{a} + \bar{b}) + \bar{c} = \bar{a}(\bar{b} + \bar{c}))$;
3. $(\forall \bar{a}, \bar{b})(\exists \bar{c})(\bar{a} + \bar{c} = \bar{b})$;
4. $(\forall \bar{a}, \bar{b})(\forall \lambda)(\lambda(\bar{a} + \bar{b}) = \lambda\bar{a} + \lambda\bar{b})$;
5. $(\forall \alpha, \beta)(\forall \bar{a})((\lambda + \beta)\bar{a} = \lambda\bar{a} + \beta\bar{a})$;
6. $(\forall a)(1 \cdot \bar{a} = \bar{a})$;
7. $(\forall \alpha, \beta)(\forall a)(\lambda(\beta\bar{a}) = (\lambda\beta)\bar{a})$.

Вектор $\bar{\theta} = (0, 0, \ldots, 0)$ є нульовим елементом.

<u>Означення 5</u>. Множина всіх *n*- вимірних векторів над полем дійсних чисел *R*, в якій введені операції додавання векторів та множення векторів на дійсні числа і виконуються вимоги 1-7 називається *n*- вимірним арифметичним векторним простором.

<u>Означення 6</u>. Нехай $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_k$ - n- вимірні вектори і $\lambda_1, \lambda_2, \ldots, \lambda_k$ – дійсні числа. Вектор $\bar{b} = \lambda_1 \bar{a}_1 + \lambda_2 \bar{a}_2 + \ldots + \lambda_k \bar{a}_k$ називається лінійною комбінацією векторів $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_k$.

<u>Означення 7.</u> Множина векторів $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_k$ називається лінійно залежною, якщо векторна рівність

$$\lambda_1 \bar{a}_1 + \lambda_2 \bar{a}_2 + \ldots + \lambda_k \bar{a}_k = \bar{\theta} \qquad (1)$$

виконується тоді, коли один з коефіцієнтів $\lambda_1, \lambda_2, \ldots, \lambda_k$ відмінний від нуля.

<u>Означення 8.</u> Множина векторів $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_k$ називається лінійно незалежною, якщо векторна рівність виконується лише тоді, коли всі коефіцієнти $\lambda_1, \lambda_2, \ldots, \lambda_k$ дорівнюють нулеві.

Теорема 1. Множина векторів $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_k$ є лінійно залежною тоді і тільки тоді, коли хоч один вектор цієї множини є лінійною комбінацією решти векторів.

Необхідність. Припустимо, що множина векторів $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_k$ є лінійно залежною. Це означає, що принаймні один з коефіцієнтів в (1) відмінний від нуля. Нехай $\lambda_1 \neq 0$. Тоді з (1) отримаємо: $\bar{a}_1 = \left(-\frac{\lambda_2}{\lambda_1}\right)\bar{a}_2 + \left(\frac{\lambda_3}{\lambda_1}\right)\bar{a}_3 + \ldots + \left(\frac{\lambda_k}{\lambda_1}\right)\bar{a}_k$

Достатність. Припустимо, що вектор $\bar{a}_1$ є лінійною комбінацією інших векторів $\bar{a}_1 = \beta_1 \bar{a}_2 + \beta_2 \bar{a}_3 + \ldots + \beta_k \bar{a}_k$. Звідси слідує:

$$\bar{a}_1 + (-\beta_1 \bar{a}_2) + (-\beta_2 \bar{a}_3) + \ldots + (-\beta_k \bar{a}_k) = \bar{\theta}.$$

Так як коефіцієнт при $\bar{a}_1$ дорівнює $1 \neq 0$, то з означення 7 слідує, що множина векторів є лінійно залежною.

Серед інших теорем відмітимо:

Теорема 2 (Штейніца). Нехай дано дві множини векторів

$$\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_k \qquad (2)$$

$$\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_k, \bar{b}_{k+1} \qquad (3)$$

Якщо кожний вектор множини (3) є лінійною комбінацією векторів множини (2), то множина векторів (2) є лінійно залежною.

Теорема 3. Кожна множина векторів, яка містить $\bar{\theta}$ є лінійно залежною.

Теорема 4. Кожна множина одиничних векторів $\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_n$ є лінійно незалежною.

<u>Означення 9.</u> Множина векторів:

$$\bar{a}_1 = (\alpha_{11}, \alpha_{12}, \alpha_{13}, \ldots, \alpha_{1n}),\ \alpha_{11} \neq 0$$

$$\bar{a}_2 = (0, \alpha_{22}, \alpha_{23}, \ldots, \alpha_{2n}),\ \alpha_{22} \neq 0$$

$$\bar{a}_3 = (0, 0, \alpha_{33}, \ldots, \alpha_{3n}),\ \alpha_{33} \neq 0$$

$$\ldots$$

$$\bar{a}_k = (0, 0, \ldots, 0, \alpha_k, \ldots, \alpha_{kn}),\ \alpha_{kk} \neq 0$$

називається діагональною множиною векторів.

Теорема 5. Діагональна множина векторів є лінійно незалежною.

Розглянемо множину векторів $M=\{\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_k\}$

<u>Означення 10.</u> Максимальне число лінійно незалежних векторів множини M називається рангом цієї множини.

<u>Означення 11.</u> Якщо ранг множини векторів M дорівнює r, то будь-який набір r лінійно незалежних векторів з M називається базисом M.

Теорема 6. Набір лінійно незалежних векторів $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_r$ множини M буде базисом M тоді і тільки тоді, коли кожний вектор множини M буде лінійною комбінацією векторів $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_r$.

Необхідність. Нехай лінійно незалежні вектори $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_r$ утворюють базис множини M. Отже, за означенням кожна множина $r+1$ вектора $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_r$ $(i=\overline{r+1,k})$ буде лінійно незалежною:

$$\lambda_1 \bar{a}_1 + \lambda_2 \bar{a}_2 + \ldots + \lambda_r \bar{a}_r + \beta \bar{a}_i = \bar{\theta}, \qquad (4)$$

причому $\beta \neq 0$. Якби $\beta=0$, то ця рівність $\lambda_1 \bar{a}_1 + \lambda_2 \bar{a}_2 + \ldots + \lambda_r \bar{a}_r = \bar{\theta}$, $\sum_{i=1}^{r} \lambda_i^2 \neq 0$ означала б, що вектори $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_r$ є лінійно залежні. З (4) отримуємо $\bar{a}_i = \left(-\frac{\lambda_1}{\beta}\right)\bar{a}_1 + \left(\frac{\lambda_2}{\beta}\right)\bar{a}_2 + \ldots + \left(\frac{\lambda_r}{\beta}\right)\bar{a}_r$.

Достатність. Нехай кожний вектор $\bar{a}_i$ з множини *M* є лінійною комбінацією лінійно незалежних векторів $\bar{a}_i = \lambda_1 \bar{a}_1 + \lambda_2 \bar{a}_2 + \ldots + \lambda_r \bar{a}_r$. Тоді кожна множина з *(r+1)* векторів буде лінійно незалежною (згідно теореми 2). Отже, множина *M* не може містити більше, ніж *r* лінійно незалежних векторів, тобто її ранг дорівнює *r* і вектори $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_r$ утворюють базис.

<u>Означення 11.</u> Перетворення множини векторів, які не змінюють її ранг, називаються еквівалентними перетвореннями.

Основними теоремами про еквівалентні перетворення множини векторів є:

Теорема 7. Якщо до множини векторів приєднати або вилучити вектор, який є їх лінійною комбінацією, то від цього ранг новоутвореної множини векторів не змінюється.

Теоремою 8. Еквівалентними перетвореннями множини векторів будуть:

1) множення будь-якого вектора на відмінне від нуля число;

2) додавання до будь-якого вектора іншого вектора, помноженого на відмінне від нуля число.

На практиці для знаходження рангу множину векторів потрібно, використовуючи теореми 7, 8, звести множину векторів до діагонального чи ступінчатого виду або скласти матрицю з компонентів векторів та звести її еквівалентними перетвореннями до діагональної чи ступінчатої форми.

Вправи.

1. Знайти ранг і базис множини векторів:

   а) $\bar{a}_1$=(1, 2, 3, 4), $\bar{a}_2$=(2, 3, 4, 5), $\bar{a}_3$=(3, 4, 5, 6);

   б) $\bar{a}_1$=(12, 3, -4), $\bar{a}_2$=(2, 3, -4, 1), $\bar{a}_3$=(4, 2, -6, 2), $\bar{a}_4$=(3, 2, 4, 1.

2. Довести теореми 7, 8.

Лекція 10. Критерії сумісності системи лінійних рівнянь. Теорема про існування ненульового розв'язку лінійної однорідної системи рівнянь, яка містить *n* рівнянь і *n+1* невідому

Запишемо лінійну неоднорідну систему рівнянь у векторній формі

$$x_1\overline{p_1}+x_2\overline{p_2}+...+x_n\overline{p_n}+=\overline{b} \qquad (1)$$

Розглянемо дві множини векторів:

$$M_1=\{\overline{p}_1,\ \overline{p}_2,...,\overline{p}_n\} \qquad (2)$$

$$M_2=\{\overline{p}_1,\ \overline{p}_2,...,\overline{p}_n,\ \overline{b}\} \qquad (3)$$

Теорема 1. Лінійна неоднорідна система рівнянь (1) сумісна тоді і тільки тоді, коли ранг множини векторів M_1 дорівнює рангу множини векторів M_2.

Необхідність. Припустимо, що система рівнянь (1) сумісна. Нехай вектор $\overline{a}=(\alpha_1, \alpha_2,...,\alpha_n)$ є її розв'язком, тобто $\lambda_1\overline{p_1}+\lambda_2\overline{p_2}+...+\lambda_n\overline{p_n}+=\overline{b}$

Ми знаємо, якщо до множини векторів приєднати вектор, який є їх лінійною комбінацією, то від цього ранг новоутвореної множини векторів не зміниться, тобто $r_{M_1}=r_{M_2}$.

Достатність. Нехай $r_{M_1}=r_{M_2}=r\le n$. Припустимо, що вектори $\overline{p}_1$, $\overline{p}_2,\ldots,\overline{p}_r$ утворюють базис множини M_1. Так як множина M_2 також містить вектори $\overline{p}_1$, $\overline{p}_2,\ldots,\overline{p}_r$, то вони будуть базис і в множині M_2. Значить множина векторів $\overline{p}_1$, $\overline{p}_2,\ldots,\overline{p}_r$, $\overline{b}$ є лінійно залежною:

$$\lambda_1\overline{p_1}+\lambda_2\overline{p_2}+...+\lambda_r\overline{p_r}+\beta\cdot\overline{b}=\overline{\theta}, \qquad (4)$$

причому $\beta\neq 0$.

Якщо припустити, що $\beta=0$, то з (4) отримаємо, що вектори $\overline{p}_1$, $\overline{p}_2,\ldots,\overline{p}_r$ є лінійно незалежні. З (4) отримаємо

$$\overline{b}=\left(-\frac{\alpha_1}{\beta}\right)\overline{p}_1+\left(\frac{\alpha_2}{\beta}\right)\overline{p}_2+...+\left(\frac{\alpha_r}{\beta}\right)\overline{p}_r \qquad (5)$$

Порівнявши (4) і (5) переконуємося, що вектор $\bar{a} = \left(-\frac{\alpha_1}{\beta}, -\frac{\alpha_2}{\beta}, ..., -\frac{\alpha_r}{\beta}, 0, 0, ..., 0 \right)$ є розв'язком системи (1).

Зауваження. Якщо розглянути систему рівнянь у виді

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = b_1 \\ a_{21}x_2 + a_{22}x_2 + ... + a_{2n}x_n = b_2 \\ \quad . \; . \; . \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n = b_m \end{cases} \tag{6}$$

і позначити через A та A_1 основну та розширену матриці системи, то теорему 1 можна сформулювати так.

Теорема 1′. Лінійна неоднорідна система рівнянь сумісна тоді і тільки тоді, коли ранг основної матриці A дорівнює рангу розширеної матриці A_1.

Саме в такому формулюванні ця теорема відома як теорема Кронеккера Канеллі.

Теорема 2. Кожна система n однорідних лінійних рівнянь, яка містить $n+1$ невідому має і причому ненульові розв'язки.

Доведення. Запишемо лінійну однорідну систему рівнянь у векторній формі

$$x_1\overline{p_1} + x_2\overline{p_2} + ... + x_n\overline{p_n} + x_{n+1}\overline{p}_{n+1} = \bar{\theta} \tag{7}$$

Розглянемо дві множини векторів

$$\bar{p}_1,\ \bar{p}_2,\ \ldots,\ \bar{p}_n,\ \bar{p}_{n+1} \tag{8}$$

$$\bar{e}_1,\ \bar{e}_2,\ \ldots,\ \bar{e}_n \tag{9}$$

Причому $\bar{e}_1,\ \bar{e}_2,\ \ldots,\ \bar{e}_n$ - одиничні n-вимірні вектори. Так як кожний вектор множини (8) є лінійною комбінацією векторів множини (9), то згідно теореми Штейніца множина (8) є лінійно залежною. Значить,

$$\alpha_1\overline{p_1} + \alpha_2\overline{p_2} + ... + \alpha_n\overline{p_n} + \alpha_{n+1}\overline{p}_{n+1} = \bar{\theta}\ , \quad \sum_{i=1}^{n+1}\alpha_i^2 \neq 0\,,$$

тобто $\bar{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{m+1})$ є ненульовий вектор системи рівнянь (7).

Лекція 11. Означення та основні властивості визначників. Необхідні і достатні умови рівності визначника нулеві

Розглянемо матрицю розмірності $n \times n$.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ & \dots & & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

<u>Означення.</u> Визначником (детермінантом) n-го порядку матриці A називається алгебраїчна сума $n!$ доданків, кожний з яких є добутком n елементів, взятих по одному і тільки одному разу з кожного рядка і кожного стовпця; знак доданка визначається множником $(-1)^t$, де t – число інверсій підстановки, яка складена з індексів доданка.

Це означення аналогічне до означення визначника 3-го порядку. Визначник n-го порядку матриці A позначають так:

$$det\, A = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ & \dots & & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Символічно визначник матриці A записують

$$det\, A = \sum_{n!} (-1)^t a_{1\alpha_1} \cdot a_{2\alpha_2} \cdot \ldots \cdot a_{n\alpha_n},$$

де t- число інверсій підстановки $\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$.

З означення визначника випливають такі основні властивості:

<u>Властивість 1.</u> Якщо у визначнику n-го порядку поміняти місцями рядки і стовпці, то визначник при цьому не зміниться.

Звідси, випливає, що всі властивості, які справджуються для рядків, будуть істинними і для стовпців.

<u>Властивість 2.</u> Якщо у визначнику n-го порядку поміняти місцями будь-які два рядки, то визначник поміняє знак на протилежний.

Властивість 3. Якщо визначник n-го порядку має два однакових рядки, то він дорівнює нулеві.

Властивість 4. Якщо кожний елемент визначника n-го порядку помножити на одне і те саме ненульове число m, то і визначник n-го порядку при цьому помножиться на число m.

Властивість 5. Якщо визначник n-го порядку має два пропорціональні рядки, то він дорівнює нулеві.

Властивість 6. Якщо кожний елемент i-го рядка є сумою двох доданків, то визначник n-го порядку дорівнює сумі двох визначників n-го порядку.

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ & \dots & & \\ a_{i_1}+b_{i_1} & a_{i_2}+b_{i_2} & \dots & a_{i_n}+b_{i_n} \\ & \dots & & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ & \dots & & \\ a_{i1} & a_{i2} & \dots & a_{in} \\ & \dots & & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ & \dots & & \\ b_{i1} & b_{i2} & \dots & b_{in} \\ & \dots & & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Властивість 7. Якщо до елементів i-го рядка додати елементи j-го рядка, помножені на одне й те саме число m, то визначник n-го порядку не змінюється.

Властивість 8. Якщо один з рядків визначника є лінійною комбінацією інших рядків, то такий визначник дорівнює нулеві.

Властивість 9. Сума добутків елементів i-го рядка на алгебраїчні доповнення елементів j-го рядка визначника n-го порядку дорівнює нулеві.

Теорема 1. Якщо всі елементи i-го рядка крім одного n-го порядку дорівнюють нулеві, то визначник n-го порядку дорівнює добутку ненульового елемента на його алгебраїчне доповнення.

Теорема 2. Визначник n-го порядку дорівнює сумі добутків елементів i-го рядка на їх алгебраїчні доповнення.

Доведемо, наприклад, теорему 2. Представимо кожний елемент a_{ij} i-го рядка у вигляді суми $a_{ij}=0+0+\ldots+a_{ij}+0+\ldots+0$. Одержимо

$$\Delta=\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ & \cdot\ \cdot\ \cdot & & \\ a_{i_1}+0+..+0 & 0+a_{i_2}+0+\dots+0 & \dots & 0+0+\dots+0+a_{i_n} \\ & \cdot\ \cdot\ \cdot & & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Представимо цей визначник *n*-го порядку як суму *n* визначників *n*-го порядку. В кожному з *n* визначників *n*-го порядку всі елементи *i*-го рядку дорівнюють *0* крім одного і згідно властивості 9 одержимо, що

$\Delta=a_{i1}A_{i1}+a_{i2}A_{i2}+\dots+a_{in}A_{in}$.

Теорема 3. Якщо рядки визначника *n*-го порядку утворюють лінійно незалежну систему, то він не дорівнює нулеві.

Теорема 4. Визначник *n*-го порядку дорівнює нулеві тоді і тільки тоді, коли його рядки є лінійно залежні.

Необхідність. Якщо визначник *n*-го порядку дорівнює нулеві, то його рядки не можуть утворювати лінійно незалежну систему. Значить, між рядками існує лінійна залежність.

Достатність. Якщо рядки визначника *n*-го порядку є лінійно залежні, то принаймні один з них є лінійною комбінацією інших і згідно з властивістю 8 він дорівнює нулеві.

Лекція 12. Знаходження оберненої матриці за допомогою елементарних перетворень та за допомогою алгебраїчних доповнень. Матричний спосіб розв'язування лінійних рівнянь

<u>Означення 1</u>. Квадратна матриця A^{-1} n-го порядку називається оберненою до квадратної матриці A n-го порядку, якщо

$$A \cdot A^{-1} = A^{-1} \cdot A = E$$

Нагадаємо, що еквівалентними перетвореннями матриці є:

1. множення будь-якого рядка (стовпця) на відмінне від 0 число c;

2. заміна місцями будь-яких двох рядків (стовпців);

3. додавання до будь-якого рядка (стовпця) іншого рядка (стовпця) помноженого на нульове число c;

<u>Означення 2</u>. Елементарною матрицею n-го порядку називається матриця, яка утворюється з одиничної матриці n-го порядку за допомогою елементарного (еквівалентного) перетворення.

Справджуються такі теореми.

Теорема 1. Заміна місцями i-го та j-го рядків матриці A еквівалентне множенню матриць A зліва на елементарну матрицю, яка отримується з одиничної матриці заміною місцями i-го та j-го рядків.

Теорема 2. Множення i-го рядка матриці A на ненульове число c еквівалентне множенню матриці A зліва на елементарну матрицю, яка отримується з одиничної множенням i-го рядка на дане число c.

Теорема 3. Додавання i-го рядка до j-го рядка, помноженого на ненульове число c еквівалентне множенню матриці A зліва на елементарну матрицю, яка отримується з одиничної матриці додаванням до i-го рядка j-го рядка, помноженого на ненульове число c.

Доведення теорем проводиться безпосереднім виконанням операцій, які вказані в теоремах.

Аналогічні теореми справджуються і з перетвореннями стовпців, лише множення на елементарні матриці проводиться справа.

<u>Теорема 4.</u> Якщо за допомогою елементарних перетворень рядків (стовпців) квадратну матрицю A можна перевести в одиничну матрицю, то за допомогою цих самих елементарних перетворень одинична матриця E перейде в матрицю A^{-1}, якщо буде оберненою до матриці A.

Доведення. Нехай за допомогою елементарних перетворень $a_1, a_2, \dots, a_k$ рядків матриці квадратна матриця A переводиться в одиничну матрицю E. Згідно теорем 1-3 перетворення a_1 переводить матрицю A в $E_{a_1} \cdot A$, перетворення a_2 переводить матрицю $E_{a_1} \cdot A$ в $E_{a_2}(E_{a_1} \cdot A)$ і т. д. Нарешті a_k переводить матрицю $E_{a_{k-1}}(E_{a_{k-2}} \dots E_{a_2}(E_{a_1} \cdot A))$ в матрицю $E_{a_k} \cdot (E_{a_{k-2}} \dots E_{a_1} A) = E$. Звідси $(E_{a_k} \dots E_{a_1})(A \cdot A^{-1}) = E \cdot A^{-1}$ або $(E_{a_1} \dots E_{a_1} A)A^{-1} = A^{-1}$, тобто $E_{a_1} E_{a_2} \dots E_{a_k} У = A^{-1}$.

З останньої рівності випливає, що елементарні перетворення $a_1, a_2, \dots, a_k$ рядків матриці переводить одиничну матрицю E в A^{-1}.

Зауваження. На практиці обернену матрицю шукають так: записують прямокутну матрицю (A/E) і за допомогою елементарних перетворень зводять її до (E/A^{-1}).

Теорема 5. Якщо визначник квадратної матриці A n-го порядку не дорівнює нулеві, то вона має обернену матрицю A^{-1}, причому

$$A^{-1} = \frac{1}{\det} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ & \dots & & \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix},$$

де A_{ij} – алгебраїчні доповнення до елемента a_{ij} матриці A.

Доведення. Позначимо шукану обернену матрицю через $X = \{x_{ij}\}^n_{i,j=1}$.

Тоді $AX = E$ або $\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ & \dots & & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ & \dots & & \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ & \dots & & \\ 0 & 0 & \dots & 1 \end{pmatrix}$

Перемножимо матриці лівої частини та прирівняємо відповідні елементи матриць лівої та правої частини. Отримаємо:

$$
(1)\ \begin{cases}
\left.\begin{array}{c}
a_{11}x_{11}+a_{12}x_{21}+\ldots+a_{1n}x_{n1}=1\\
a_{21}x_{11}+a_{22}x_{21}+\ldots+a_{2n}x_{n1}=0\\
\ldots\\
a_{n1}x_{11}+a_{n2}x_{21}+\ldots+a_{nn}x_{n1}=0
\end{array}\right\}(1')\\
\left.\begin{array}{c}
a_{11}x_{12}+a_{12}x_{22}+\ldots+a_{1n}x_{n2}=0\\
a_{21}x_{12}+a_{22}x_{22}+\ldots+a_{2n}x_{n2}=1\\
\ldots\\
a_{n1}x_{12}+a_{n2}x_{22}+\ldots+a_{nn}x_{n2}=0
\end{array}\right\}(1'')\\
\ldots\\
\ldots\\
\ldots\\
\left.\begin{array}{c}
a_{11}x_{1n}+a_{12}x_{2n}+\ldots+a_{1n}x_{nn}=0\\
a_{21}x_{1n}+a_{22}x_{2n}+\ldots+a_{2n}x_{nn}=0\\
\ldots\\
a_{n1}x_{1n}+a_{n2}x_{2n}+\ldots+a_{nn}x_{nn}=1
\end{array}\right\}(1^{(n)})
\end{cases}
$$

Одержана система n^2 рівнянь з n^2 невідомими розкладається на n підсистем, кожна з яких складається з n рівнянь і n невідомих, причому визначник основної матриці кожної з підсистем є $det\ A\neq 0$. Згідно теореми Крамера кожна з n систем має і притому єдиний розв'язок. Знайдемо вираз для x_{ij}.

Обчислимо, наприклад, x_{k_1}:

$$
x_{k_1}=\frac{\Delta_{X_{K_1}}}{\det A}=\frac{\begin{vmatrix}
a_{11}\ a_{12}\ldots a_{1k-1}\ 1\ a_{1k+1}\ldots a_{1n}\\
a_{21}\ a_{22}\ldots a_{2k-1}\ 0\ a_{2k+1}\ldots a_{2n}\\
\ldots\\
a_{n1}\ a_{n2}\ldots a_{nk-1}\ 0\ a_{nk+1}\ldots a_{nn}
\end{vmatrix}}{\det A}=\frac{A_{1k}}{\det A}
$$

Аналогічно знаходимо решту x_{ij}. Безпосереднім множенням матриці A на знайдену переконуємося в тому, що знайдена матриця обернена до матриці A.

Розглянемо систему лінійних рівнянь:

$$
\begin{cases}
a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n=b_1\\
a_{21}x_2+a_{22}x_2+\ldots+a_{2n}x_n=b_2\\
\ldots\\
a_{n1}x_1+a_{n2}x_2+\ldots+a_{nn}x_n=b_n
\end{cases}
$$

Нехай

$$A=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ & \dots & & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix},\ X=\begin{pmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_n \end{pmatrix},\ B=\begin{pmatrix} b_1 \\ b_2 \\ . \\ . \\ . \\ b_n \end{pmatrix}$$

Тоді систему лінійних рівнянь можна записати у матричній формі

$$A \cdot X = B$$

Якщо матриця A має обернену матрицю A^{-1}, то помноживши обидві частини матричного рівняння зліва на A^{-1}, отримаємо

$$X = A^{-1} \cdot B$$

Безпосередньою перевіркою переконуємося, що $X=A^{-1} \cdot B$ є єдиним розв'язком лінійної системи рівнянь.

Вправи

1. Знайти двома способами обернену матрицю до матриці $A=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 6 \end{pmatrix}$.
2. Розв'язати матричним способом систему рівнянь $\begin{cases} x_1 + 2x_2 + 3x_3 = 1 \\ 2x_1 + 3x_2 + 4x_3 = 2 \\ 3x_1 + 4x_2 + 6x_3 = 3 \end{cases}$.
3. Довести теореми 1, 2, 3.

Лекція 13. Теорема Крамера

Розглянемо систему лінійних рівнянь, яка містить *n* рівнянь і *n* невідомих:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = b_1 \\ a_{21}x_2 + a_{22}x_2 + ... + a_{2n}x_n = b_2 \\ \quad . \; . \; . \\ a_{n1}x_1 + a_{n2}x_2 + ... + a_{nn}x_n = b_n \end{cases} \qquad (1)$$

Теорема. Якщо визначник основної матриці системи лінійних рівнянь (1) відмінний від нуля, то система рівнянь має єдиний розв'язок, який знаходиться за формулами Крамера.

$$x_1 = \frac{\Delta_{X_1}}{\Delta},\ x_2 = \frac{\Delta_{X_2}}{\Delta},\ \ldots,\ x_n = \frac{\Delta_{X_n}}{\Delta} \qquad (2)$$

Доведення. Домножимо перше рівняння системи (1) на алгебраїчне доповнення A_{11}, друге рівняння системи – на алгебраїчне доповнення A_{21} і т. д., нарешті, *n*-е рівняння системи - алгебраїчне доповнення A_{n1} і додамо перетворені рівняння, групуючи доданки відносно невідомих $x_1, x_2, \ldots, x_n$. Одержимо:

$$x_1\sum_{i=1}^{n} a_{i1}A_{i1} + x_2\sum_{i=1}^{n} a_{i2}A_{i1} + ... + x_n\sum_{i=1}^{n} a_{in}A_{i1} = \sum_{i=1}^{n} b_i A_{i1}$$

З властивостей визначників випливає, що сума добутків елементів *I* стовпця на свої алгебраїчні доповнення дорівнює визначникові, а сума добутків елементів *2, 3, …, n* стовпців на алгебраїчні доповнення елементів *I* стовпця дорівнює нулеві.

Маємо $x_1 \cdot \Delta = \Delta_{x_1}$. Звідси $x_1 = \frac{\Delta_{x_1}}{\Delta}$. Аналогічно отримуємо вирази $x_2 = \frac{\Delta_{x_2}}{\Delta}, \ldots, x_n = \frac{\Delta_{x_n}}{\Delta}$. Переконаємося, що знайдені значення є розв'язком лінійної системи рівнянь (1). Підставимо, наприклад, знайдені значення $x_1, x_2, \ldots, x_n$ в ліву частину першого рівняння:

$$a_{11}\frac{\Delta_{x_1}}{\Delta}+a_{12}\frac{\Delta_{x_2}}{\Delta}+\ldots+a_{1n}\frac{\Delta_{x_n}}{\Delta}=\frac{1}{\Delta}(a_{11}\Delta x_1+a_{12}\Delta x_2+...+a_{1n}\Delta x_n)=\frac{1}{\Delta}$$

$$a_{11}\sum_{i=1}^{n}b_iA_{i1}+a_{12}\sum_{i=1}^{n}b_iA_{i2}+...+a_{1n}\sum_{i=1}^{n}b_iA_{in}=\frac{1}{\Delta}\cdot\sum_{i=1}^{n}b_i\,(a_{11}A_{i1}+a_{12}A_{i2}+...+a_{1n}A_{in}=\frac{1}{\Delta}\cdot b_1\cdot\Delta=b_1$$

Аналогічно переконуємося, що знайдені $x_1, x_2, \ldots, x_n$ є розв'язком *2, 3, …, n* рівнянь.

Так як визначник основної матриці не дорівнює нулеві, то його рядки лінійно незалежні. Значить ранг основної матриці дорівнює *n*, але і ранг розширеної матриці також дорівнює *n*. Ранги рівні співпадають з кількістю невідомих. Тоді система рівнянь, згідно з теоремою Гауса, має єдиний розв'язок.

Лекція 14. Фундаментальна система розв'язків лінійної однорідної системи рівнянь. Теореми про існування фундаментальної системи розв'язків

Розглянемо лінійну однорідну систему рівнянь:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = 0 \\ a_{21}x_2 + a_{22}x_2 + ... + a_{2n}x_n = 0 \\ \quad . \; . \; . \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n = 0 \end{cases} \qquad (1)$$

Як відомо сума будь-яких двох розв'язків системи рівнянь (1) є розв'язком системи рівнянь (1) і додаток будь-якого ненульового числа на розв'язок системи рівнянь (1) є розв'язком цієї системи. Отже, множина розв'язків однорідної системи рівнянь (1) є підпростором *n*- вимірного арифметичного векторного простору. Базис цього підпростору називають ще фундаментальною системою розв'язків лінійної однорідної системи рівнянь 1.

<u>Означення.</u> Фундаментальною системою розв'язків лінійної однорідної системи рівнянь (1) називається така лінійно незалежна множина розв'язків, що всякий розв'язок системи рівнянь (1) є її лінійною комбінацією.

Теорема. Якщо ранг *Z* основної матриці системи рівнянь (1) менший кількості невідомих *n*, то існує фундаментальна система розв'язків і кількість розв'язків фундаментальної системи дорівнює *n-r*.

Доведення. Якщо *r*<*n*, то система має безліч розв'язків. Загальним розв'язком системи рівнянь (1) в цьому випадку буде:

$$M=\{(\sum_{i=r+1}^{n} q_{1i}x_i,\ \sum_{i=r+1}^{n} q_{2i}x_i,...,\ \sum_{i=r+1}^{n} q_{ri}x_i, x_{r+1},...,x_n) :\ x_{r+1}, x_{r+2},..., x_n \in R\}$$

Виберемо з загального розв'язку *n-r* розв'язків шляхом фіксування незалежних невідомих так, щоб одна з невідомих була рівна 1, а всі інші – нулеві. Отримаємо розв'язки:

$$\bar{a}_1 = (q_{1r+1}, q_{2r+1}, ..., q_{rr+1}, 1, 0, ..., 0)$$

$$\bar{a}_2 = (q_{1r+2}, q_{2r+2}, ..., q_{rr+2}, 0,1,...,0)$$

$$\cdot\cdot\cdot$$

$$\bar{a}_1 = (q_{1n}, q_{2n}, ..., q_{rn}, 0,0,...,1)$$

Покажемо, що ця множина розв'язків є лінійно незалежна і, що кожний розв'язок системи (1) є її лінійною комбінацією. Так як ця множина розв'язків містить мінор *(n-r)*-го порядку $\begin{vmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ & & \cdot\cdot\cdot & \\ 0 & 0 & ... & 1 \end{vmatrix} = 1 \neq 0$, то вона є лінійно незалежна.

Нехай $\bar{a} = (\gamma_1, \gamma_2, ..., \gamma_r, \gamma_{r+1}, ..., \gamma_n)$ є довільним розв'язком системи рівнянь (1). Перші *r* компонент вектора $\bar{a}$ виражаються через $\gamma_{r+1}, \gamma_{r+2}, ..., \gamma_n$ з загального розв'язку. Значить $\bar{a} = (\sum_{i=r+1}^{n} q_{1i}\gamma_i, \sum_{i=r+1}^{n} q_{2i}\gamma_i, ..., \sum_{i=r+1}^{n} q_{ri}\gamma_i, \gamma_{r+1}, ..., \gamma_n)$. З другої сторони помножимо вектор $\bar{a}_1$ на γ_{r+1}, $\bar{a}_2$ - γ_{r+2}, і т. д., $\bar{a}_r$ - γ_n і додамо:

$$\gamma_{r+1}\bar{a}_1 + \gamma_{r+2}\bar{a}_2 + ... + \gamma_n \bar{a}_{n-r} = (\sum_{i=r+1}^{n} q_{1i}\gamma_i, \sum_{i=r+1}^{n} q_{2i}\gamma_i, ..., \sum_{i=r+1}^{n} q_{ri}\gamma_i, \gamma_{r+1}, \gamma_{r+2} ..., \gamma_n),$$

довільний розв'язок $\bar{a}$ системи рівнянь (1) є лінійною комбінацією розв'язків $\bar{a}_1, \bar{a}_2, ..., \bar{a}_{n-r}$.

Лекція 15. Означення та приклади векторного простору. Підпростори. Основні властивості векторного простору

Розглянемо множину $\overline{V}$ елементів довільної природи і деяке поле *P*. Елементи множини $\overline{V}$ будемо позначати $\overline{a}, \overline{b}, \overline{c}, \ldots$, а елементи поля *P* - α, β, $\gamma, \ldots$. В множині $\overline{V}$ введемо операцію додавання, яка кожній впорядкованій парі $\overline{a}, \overline{b}$ елементів із $\overline{V}$ ставить у відповідність єдиний елемент $\overline{c}$ із $\overline{V}$. Означимо операцію множення елементів із $\overline{V}$ на елементи із *P*, яка кожній парі $\overline{a} \in \overline{V}$ та $\alpha \in$P ставить у відповідність лише один елемент $\overline{b}$ із $\overline{V}$: $\overline{b} = \alpha \cdot \overline{a} = \overline{a} \cdot \alpha$.

<u>Означення 1</u>. Множина $\overline{V}$ елементів довільної природи над полем *P* називається векторним простором, якщо у $\overline{V}$ введена операція додавання і множення елементів множини $\overline{V}$ на елементи поля *P* і виконуються аксіоми:

1. $(\forall \overline{a}, \overline{b})(\overline{a} + \overline{b} = \overline{b} + \overline{a})$;
2. $(\forall \overline{a}, \overline{b}, \overline{c})((\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c}))$;
3. $(\forall \overline{a}, \overline{b})(\exists \overline{x})(\overline{a} + \overline{x} = \overline{b})$;
4. $(\forall \alpha, \beta)(\forall a)(\lambda(\beta \overline{a}) = (\lambda\beta)\overline{a})$;
5. $(\forall a)(1 \cdot \overline{a} = \overline{a})$, 1 – одиниця поля *P*;
6. $(\forall \alpha, \beta)(\forall \overline{a})((\lambda + \beta)\overline{a} = \lambda\overline{a} + \beta\overline{a})$;
7. $(\forall \overline{a}, \overline{b})(\forall \lambda)(\lambda(\overline{a} + \overline{b}) = \lambda\overline{a} + \lambda\overline{b})$.

Елементи множини $\overline{V}$ називатимемо векторами, а елементи поля *P* називатимемо скалярами.

Векторними просторами будуть:

Приклади.

1. *n*-вимірний арифметичний векторний простір

2. Сукупність *c[a, b]* всіх неперервних функцій *y=φ(x),* визначених на відрізку *[a, b]* з поточковим додаванням і множенням їх на дійсні числа.

3. Сукупність $P[x]$ всіх многочленів від однієї змінної з коефіцієнтами з деякого поля P відносно операції додавання многочленів і множення многочленів на елемент поля P.

4. Сукупність всіх квадратних матриць з елементами з деякого числового поля з поелементним додаванням та множенням на число.

Перевірку аксіом векторного простору наведених прикладів рекомендуємо провести самостійно.

З означення векторного простору випливають такі основні властивості:

<u>Означення 2.</u> Вектор $\bar{\theta}$ називається нульовим вектором, якщо $(\underset{\bar{V}}{\forall}\bar{a})(\bar{a}+\bar{\theta}=\bar{a})$.

1. В просторі $\bar{V}$ існує єдиний нульовий вектор.

Нехай $\bar{a}\in\bar{V}$. За аксіомою 3 рівняння $(\bar{a}+\bar{x}=\bar{a})$ має розв'язок. Позначимо його - $\bar{\theta}$. Вектор $\bar{\theta}$ буде нульовим вектором, якщо для будь-якого вектора $\bar{b}\in\bar{V}$ $(\bar{b}+\bar{\theta}=\bar{b})$. З аксіоми 3 випливає, що рівняння $(\bar{a}+\bar{y}=\bar{b})$ має розв'язок. Тоді $\bar{b}+\bar{\theta}=(\bar{a}+\bar{y})+\bar{\theta}=(\bar{a}+\bar{\theta})+\bar{y}=(\bar{a}+\bar{y})=\bar{b}$. Єдиність випливає з таких міркувань. Нехай існують два різні нульові вектори $\bar{\theta}_1$ та $\bar{\theta}_2$. Тоді

$$\left.\begin{array}{l}\bar{\theta}_1+\bar{\theta}_2=\bar{\theta}_1\\ \bar{\theta}_1+\bar{\theta}_2=\bar{\theta}_2\end{array}\right|\Rightarrow\bar{\theta}_1=\bar{\theta}_2,$$

що й доводить єдиність нульового вектора.

<u>Означення 3</u>. Вектор $-\bar{a}$ називається протилежним до вектора $\bar{a}$, якщо $\bar{a}+(-\bar{a})=\bar{\theta}$.

2. Для кожного вектора $\bar{a}$ існує єдиний протилежний вектор $-\bar{a}$.

Існування вектора $-\bar{a}$ випливає з аксіоми 3 для векторів $\bar{a}$ та $\bar{\theta}$. Припустимо, що вектор $\bar{a}$ має два протилежні вектори $\bar{x}$ та $\bar{y}$. Тоді $\bar{a}+\bar{x}=\bar{\theta}$, $\bar{a}+\bar{y}=\bar{\theta}$, $\bar{y}=\bar{y}+\bar{\theta}=\bar{y}+(\bar{a}+\bar{x})=(\bar{y}+\bar{a})+\bar{x}=\bar{\theta}+\bar{x}=\bar{x}$. Що й доводить єдиність протилежного вектора.

Зауваження. При доведенні єдиності нульового вектора, єдиності протилежного вектора використаємо метод доведення від супротивного в інтерпретації $a \Rightarrow b \Leftrightarrow a \wedge \bar{b} \Rightarrow b$.

3. $(\forall \bar{a})(0 \cdot \bar{a} = \bar{\theta})$

Справді $\bar{a} = (1+0)\ \bar{a} = 1 \cdot \bar{a} + 0 \cdot \bar{a} = \bar{a} + 0 \cdot \bar{a}$ або $\bar{a} = \bar{a} + 0 \cdot \bar{a}$ або $0 \cdot \bar{a} = \bar{\theta}$

4. $(\forall \alpha)(\alpha \cdot \bar{\theta} = \bar{\theta})$

Для довільного $\bar{a} \in \bar{V}$, $\alpha \bar{a} = \alpha(\bar{a} + \bar{\theta}) = \alpha \bar{a} + \alpha \cdot \bar{\theta}$ *або* $\alpha \bar{a} = \alpha \bar{a} + \alpha \cdot \bar{\theta}$ *або* $\alpha \cdot \bar{\theta} = \bar{\theta}$

5. $(\forall \bar{a})((-1) \cdot \bar{a} = \bar{a})$

Ця властивість випливає з рівностей $\bar{\theta} = 0 \cdot \bar{a} = (1-1)\ \bar{a} = 1 \cdot \bar{a} + (-1)\ \bar{a} = \bar{a} + (-1)\ \bar{a}$ та єдиності протилежного вектора.

6. $(\forall \bar{a})(-(-\bar{a}) = \bar{a})$

<u>Означення 4</u>. Підмножина $\bar{U}$ векторного простору $\bar{V}$ називається підпростором простору $\bar{V}$, якщо $\bar{U}$ є простором відносно тих самих операцій додавання векторів та множення векторів на скаляри.

Очевидно, що й буде підпростором $\bar{V}$ тоді і тільки тоді, коли:

1. $(\underset{\bar{U}}{\forall} \bar{a}, \bar{b})((\bar{a} + \bar{b}) \in \bar{U})$;

2. $(\underset{\bar{U}}{\forall} \bar{a})(\underset{P}{\forall} \alpha)(\alpha \bar{a} \in \bar{U})$.

Підпростір $\bar{U}$ містить нульовий вектор. З 2 випливає, що $(\underset{\bar{U}}{\forall} a)\ (0 \cdot \bar{a} \in \bar{U})$ але $0 \cdot \bar{a} = \bar{\theta}$.

<u>Означення 4.</u> Перетином двох підпросторів $\bar{U}$ та $\bar{W}$ векторного простору $\bar{V}$ називається сукупність усіх векторів, які належать одночасно і $\bar{U}$ і $\bar{W}$. Перетин підпросторів позначають $\bar{U} \cap \bar{W}$.

З означення 4 випливає, що перетин двох підпросторів є підпростір.

<u>Означення 5.</u> Сумою $\bar{U} + \bar{W}$ двох підпросторів векторного простору $\bar{V}$ називається сукупність векторів виду $\bar{u} + \bar{w}$, де $\bar{u}$ - будь-який вектор з $\bar{U}$, а $\bar{w}$ - будь-який вектор з $\bar{W}$.

Так як сума підпросторів є замкнутою відносно операцій додавання векторів та множення векторів на скаляр, то вона є підпростором.

<u>Означення 6.</u> Об'єднанням двох підпросторів $\overline{U}$ і $\overline{W}$ векторного простору $\overline{\mathrm{V}}$ називається сукупність векторів цього простору, які належать хоча б одному з розглянутих підпросторів і позначають $\overline{U} \cup \overline{W}$.

Об'єднання двох підпросторів взагалі кажучи не є підпростором. Наприклад, об'єднання одновимірних підпросторів, які складаються з векторів осей *Ox, Oy* не є підпростором.

Відмітимо, ще дві теореми про підспростори.

Теорема 1. Якщо $\overline{U}, \overline{W}$ підпростори векторного простору $\overline{V}$, то

$$dim\,(\overline{U} + \overline{W}) + dim\,\overline{U} \cap \overline{W} = dim\,\overline{U} + dim\,\overline{W}.$$

Теорема 2. Якщо $dim\,\overline{U} = r,\ dim\,\overline{W} = t$ і $r + t > dim\,\overline{\mathrm{V}}$, то $\overline{U}$ і $\overline{W}$ мають спільні вектори, які відмінні від нульового вектора.

Лекція 16. Базис та розмірність скінченновимірного векторного простору. Ізоморфізм векторних просторів

Будемо вважати, що елементи поля P є числа (наприклад, поле R, Q, C і т. д.). Всі можливі векторні простори можна поділити на два типи.

1. Простори, в яких є лінійно незалежна система векторів, яка складається з n векторів, але немає лінійно незалежної системи з більшою кількістю векторів.

2. Простори, в яких є лінійно незалежні системи, які складаються з як завгодно великої кількості векторів.

<u>Означення 1.</u> Векторний простір $\overline{V}$ називається скінченновимірним, якщо в ньому існує лінійно незалежна система, що складається з n векторів і кожна система векторів, що складається з $n+1$ вектора – лінійно незалежна.

Це означення вважають за аксіому вимірності. Векторні простори, в яких виконується аксіома вимірності називають ще n- вимірним або простором вимірності n. Якщо вимірність простору $\overline{V}$ дорівнює n, то це позначають так $dim\ \overline{V} = n$, а сам простір позначають $\overline{V}_n$.

<u>Означення 2.</u> Базисом векторного простору $\overline{V}$ називається лінійно незалежна сукупність векторів $\overline{a}_1$, $\overline{a}_2$, …, $\overline{a}_m$ і таких, що кожний вектор $\overline{a}$ з $\overline{V}$ є їх лінійною комбінацією.

При цьому вважаємо, що базис – це сукупність векторів, які взяті у певному порядку.

Теорема 1. Якщо $\overline{V}_n$ – n- вимірний векторний простір, то кожна сукупність n лінійно незалежних векторів утворює базис $\overline{V}_n$.

Доведення. Нехай $\overline{a}_1$, $\overline{a}_2$, …, $\overline{a}_n$ – будь-яка лінійно незалежна сукупність векторів з $\overline{V}_n$. Покажемо, що кожний вектор $\overline{a} \in \overline{V}_n$ є їх лінійною комбінацією. Множина $n+1$ векторів $\overline{a}_1$, $\overline{a}_2$, …, $\overline{a}_n$, $\overline{a}$ є лінійно залежною. Отже,

$$\lambda_1 \overline{a}_1 + \lambda_2 \overline{a}_2 + \ldots + \lambda_n \overline{a}_n + \lambda \overline{a} = \overline{\theta} \qquad (1)$$

причому хоч би один з скалярів відмінний від нуля. покажемо, що $\lambda \neq 0$. Справді, якщо припустити, що $\lambda=0$, тоді з векторної рівності $\lambda_1 \bar{a}_1 + \lambda_2 \bar{a}_2 + \ldots + \lambda_n \bar{a}_n + \lambda \bar{a} = \bar{\theta}$ і того, що хоч один з скалярів $\lambda_i \neq 0$ випливає, що сукупність векторів $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n$ є лінійно залежною, а це суперечить умові теореми. З (1) випливає, що $\bar{a} = (-\frac{\lambda_1}{\lambda})\bar{a}_1 + (-\frac{\lambda_2}{\lambda})\bar{a}_2 + \ldots + (-\frac{\lambda_n}{\lambda})\bar{a}_n$, що й треба було довести.

Теорема 2. Якщо у векторному просторі $\bar{V}$ є базис, який складається з n векторів, то простір $\bar{V}$ має вимірність n.

Нехай $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n$ є базисом простору $\bar{V}$. Доведемо, що будь-які $n+1$ векторів простору $\bar{V}$ лінійно залежні. Виберемо будь-які $n+1$ векторів простору $\bar{V}$ $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n, \bar{b}_{n+1}$. Кожний з цих векторів є лінійною комбінацією векторів базису, тобто

$$\bar{b}_i = \sum_{k=1}^{n} \alpha_{ik} \bar{a}_k \qquad (i = \overline{1, n+1}) \tag{2}$$

Розглянемо сукупність n-вимірних арифметичних векторів

$$\bar{c}_1 = (\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1n})$$

$$\bar{c}_2 = (\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2n})$$

$$\ldots$$

$$\bar{c}_n = (\alpha_{n1}, \alpha_{n2}, \ldots, \alpha_{nn})$$

$$\bar{c}_{n+1} = (\alpha_{n+11}, \alpha_{n+12}, \ldots, \alpha_{n+1n})$$

З теореми Штейніца випливає, що сукупність векторів $\bar{c}_1, \bar{c}_2, \ldots, \bar{c}_n, \bar{c}_{n+1}$ є лінійно залежною, тобто

$$\lambda_1 \bar{c}_1 + \lambda_2 \bar{c}_2 + \ldots + \lambda_{n+1} \bar{c}_{n+1} = \bar{\theta} \tag{3}$$

і принаймні один із скалярів $\lambda_i \neq 0$. З (3) випливають рівності $\sum_{i=1}^{n+1} \lambda_i \alpha_{ik}, \quad k = \overline{1, n}$

Розглянемо тепер лінійну комбінацію $\sum_{i=1}^{n+1} \lambda_i \bar{b}_i$. З (2) і (3) випливає, що

$$\sum_{i=1}^{n+1} \lambda_i \bar{b}_i = \sum_{i=1}^{n} \lambda_i (\sum_{k=1}^{n} \alpha_{ik} \bar{a}_k) = \sum_{k=1}^{n} (\sum_{i=1}^{n+1} \lambda_i \alpha_{ik}) \bar{a}_k = \bar{\theta},$$

а це й означає, що система векторів $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n, \bar{b}_{n+1}$ – лінійно незалежна.

Наслідок. Кожний базис *n*- вимірного простору $\bar{V}_n$ складається з *n* векторів.

<u>Означення 3.</u> Векторні простори $\bar{V}$, $\bar{W}$ задані над одним і тим самим полем *P* називаються ізоморфними, якщо між їх векторами можна встановити взаємно однозначну відповідність і таку, що коли вектору $\bar{a} \in \bar{V}$ відповідає вектор $\bar{a}_1 \in \bar{W}$, вектору $\bar{b} \in \bar{V}$ відповідає вектор $\bar{b}_1 \in \bar{W}$, то вектору $(\bar{a} + \bar{b}) \in \bar{V}$ відповідає вектор $(\bar{a}_1 + \bar{b}_1) \in \bar{W}$ і $\lambda\bar{a} \to \lambda\bar{a}_1$.

Сама взаємно однозначна відповідність називається ізоморфізмом. Так як векторний простір відносно операції додавання векторів є абелевою групою, то очевидно, що при ізоморфізмі нульовий вектор $\bar{\theta} \in \bar{V}$ переходить в нульовий вектор $\bar{\theta}_1 \in \bar{W}$.

Теорема 3. Кожний *n*-вимірний векторний простір ізоморфний *n*-вимірному арифметичному векторному простору.

Доведення. Виберемо в $\bar{V}_n$ будь-який базис *B*. $B=\{\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n\}$. Виберемо $\bar{a} \in \bar{V}$. Розкладемо вектор $\bar{a}$ за базисом *B*

$$\bar{a} = \xi_1\bar{a}_1 + \xi_2\bar{a}_2 + \ldots + \xi_n\bar{a}_n$$

Вектору $\bar{a} \in \bar{V}_n$ співставимо *n*- вимірний арифметичний вектор $\bar{\xi} = (\xi_1, \xi_2, \ldots, \xi_n)$. Очевидно, що така відповідність буде взаємно однозначною. Вектор $\lambda\bar{a} = (\lambda\xi_1)\bar{a}_1 + (\lambda\xi_2)\bar{a}_2 + \ldots + (\lambda\xi_n)\bar{a}_n$ перейде у вектор $\lambda\bar{\xi} = (\lambda\xi_1, \lambda\xi_2, \ldots, \lambda\xi_n)$, тобто вектору $\lambda\bar{a}$ відповідає вектор $\lambda\bar{\xi}$. Розглянемо ще вектор $\bar{b} \in \bar{V}_n$. $\bar{b} = r_1\bar{a}_1 + r_2\bar{a}_2 + \ldots + r_n\bar{a}_n$. Йому відповідає вектор $\bar{r} = (\bar{r}_1, \bar{r}_2, \ldots, \bar{r}_n)$,

$$\bar{a} + \bar{b} = (\bar{\xi}_1 + r_1)\,\bar{a}_1 + (\bar{\xi}_2 + r_2)\,\bar{a}_2 + \ldots + (\bar{\xi}_n + r_n)\,\bar{a}_n$$

Отже, вектору $\bar{a} + \bar{b}$ відповідає вектор з компонентами $\xi_1 + r_1, \xi_2 + r_2, \ldots, \xi_n + r_n$, тобто вектор $\bar{a} + \bar{b}$ переходить у вектор $\bar{\xi} + \bar{r}$.

Теорема 4. Усі векторні простори, які мають однакову вимірність *n*, ізоморфні між собою.

Лекція 17. Лінійні оператори. Власні значення і власні вектори лінійного оператора

Означення 1. Нехай U і V – векторні простори над полем P і A: $U \to V$ – відображення, яке кожному вектору $u \in U$ зіставляє вектор $Au \in V$. Відображення A називається лінійним відображенням або гомоморфізмом простору U у простір V, якщо воно задовольняє умовам лінійності:

1) $\forall \underset{V}{u_1} \forall \underset{V}{u_2} \left(\mathrm{A}(u_1 + u_2) = \mathrm{A}u_1 + \mathrm{A}u_2\right)$,

2) $\forall \underset{P}{\alpha} \forall \underset{V}{u} \left(\mathrm{A}(\alpha u) = \alpha \mathrm{A}u\right)$.

Лінійне відображення векторного простору U в себе називається ліійним оператором простору U.

З умов 1) і 2) випливає, що для будь-яких $u_1, ..., u_n \in U$ і $\alpha_1, \alpha_2, ..., \alpha_n \in P$ $\mathrm{A}(\alpha_1 u_1 + ... + \alpha_n u_n) = \alpha_1 \mathrm{A}u_1 + ... + \alpha_n \mathrm{A}u_n$. Також легко встановлюються рівності $\mathrm{A}0 = 0$ і $\mathrm{A}(-u) = -\mathrm{A}u$. Справді, $\mathrm{A}0 = \mathrm{A}(0 \cdot u) = 0 \cdot \mathrm{A}u = 0$, $\mathrm{A}(-u) = \mathrm{A}((-1)u) = (-1)\mathrm{A}u = -\mathrm{A}u$.

Наведемо кілька прикладів лінійних відображень і лінійних операторів у векторних просторах.

Важливе значення при вивченні лінійних операторів, заданих у векторному просторі, мають підпростори, які оператором відображаються самі в себе.

Означення 2. Підпростір U векторного простору V називається інваріантним відносно лінійного оператора A, заданого в просторі V, якщо $\mathrm{A}(U) \subseteq U$, тобто якщо для будь-якого вектора $u \in U$ $\mathrm{A}u \in U$.

Очевидно, сам простір V і нульовий підпростір $\{0\}$ інваріантні відносно будь-якого лінійного оператора A, заданого в просторі V. Будь-який підпростір простору V інваріантний відносно тотожнього оператора E і нульового оператора O. Якщо у векторному просторі V заданий оператор подібності A з коефіцієнтом $\lambda \neq 0$, тобто $\mathrm{A}u = \lambda u$ для будь-якого вектора $u \in V$, то довільний одновимірний підпростір простору V, тобто підпростір, що породжується одним своїм елементом, буде інваріантним відносно оператора

подібності *A*. У векторному просторі W_2 геометричних векторів площини, в якому заданий оператор *A* повороту навколо деякої точки *O* площини на кут $\varphi \neq k\pi (k \in \mathrm{Z})$, єдиними інваріантними відносно даного оператора підпросторами є сам простір *V* і нульовий підпростір $\{0\}$. Неважко бачити, що образ *ImA* і ядро *KerA* – інваріантні підпростори відносно оператора *A*.

Займемось тепер дослідженням одновимірних інваріантних підпросторів, які відіграють особливо важливу роль при вивченні лінійних операторів. Якщо $U = \{\lambda u | \lambda \in P\}$ – одновимірний підпростір простору *V*, інваріантний відносно лінійного оператора *A*, то $\mathrm{A}u = \lambda u$ для деякого $\lambda \in P$. Тоді для довільного елемента $\alpha u \in U$ будемо мати: $\mathrm{A}(\alpha u) = \alpha \mathrm{A}u = \alpha(\lambda u) = \lambda(\alpha u)$.

Означення 3. Ненульовий вектор *u* простору *V* називається власним вектором лінійного оператора *A*, якщо $\mathrm{A}u = \lambda u$ для деякого елемента $\lambda \in P$. Елемент λ при цьому називається власним значенням оператора *A*, що відповідає власному вектору *u*. Говорять також, що власний вектор *u* належить власному значенню λ.

Якщо *u* – власний вектор лінійного оператора *A*, то існує єдиний елемент $\lambda \in P$ такий, що $\mathrm{A}u = \lambda u$. Справді, якщо $u \neq 0$, то $\lambda u = \lambda_1 u \Rightarrow (\lambda - \lambda_1)u = 0 \Rightarrow \lambda - \lambda_1 = 0 \Rightarrow \lambda = \lambda_1$. Далі, якщо *u* – власний вектор оператора *A*, що належить власному значенню λ, то для довільного ненульового елемента α з поля *P* вектор αu теж є власним вектором оператора *A*, який належить тому самому власному значенню λ. Справді, $\mathrm{A}(\alpha u) = \alpha \mathrm{A}u = \alpha(\lambda u) = \lambda(\alpha u)$. Отже, кожний власний вектор оператора *A* породжує в просторі *V* одновимірний інваріантний підпростір, всі ненульові вектори якого є власними векторами оператора *A*, що належать одному і тому ж власному значенню. Таким чином, задача знаходження інваріантних відносно оператора *A* одновимірних підпросторів простору *V* рівносильна відшуканню власних векторів оператора *A*. Таким, наприклад, є оператор повороту в просторі W_2 геометричних векторів площини на кут $\varphi \neq k\pi (k \in \mathrm{Z})$ навколо довільної точки *O* площини. З іншого боку, є оператори, для яких

кожний ненульовий вектор простору є власним. Прикладом такого оператора є оператор подібності з коефіцієнтом λ.

Теорема 1. Власні вектори $a_1, a_2, ..., a_m$ лінійного оператора *A*, які належать попарно різним власним значенням $\lambda_1, \lambda_2, ..., \lambda_m$, утворюють лінійно незалежну систему.

Доведення. Будемо доводити теорему методом математичної індукції за числом m власних векторів. При *m=1* теорема істинна, оскільки вектор a_1 ненульовий. Нехай твердження теореми справджується для довільних *m–1* власних векторів оператора *A*, що належать попарно різним власним значенням. Доведемо, що тоді довільні m власні вектори $a_1, a_2, ..., a_m$, які належать попарно різним власним значенням $\lambda_1, \lambda_2, ..., \lambda_m$, теж будуть лінійно незалежними. Справді, якщо для деяких $\alpha_1, \alpha_2, ..., \alpha_m \in P$ $\alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_m a_m = 0$, то $0 = \mathrm{A}0 = \mathrm{A}(\alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_m a_m) = \alpha_1 \mathrm{A} a_1 + \alpha_2 \mathrm{A} a_2 + ... + \alpha_m \mathrm{A} a_m = \alpha_1 \lambda_1 a_1 + \alpha_2 \lambda_2 a_2 + ... + \alpha_m \lambda_m a_m$, тобто $\alpha_1 \lambda_1 a_1 + \alpha_2 \lambda_2 a_2 + ... + \alpha_m \lambda_m a_m = 0$. Віднімаючи від останньої рівності почленно рівність $\alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_m a_m = 0$, домножену на λ_k, отримаємо: $\alpha_1(\lambda_1 - \lambda_m) a_1 + \alpha_2(\lambda_2 - \lambda_m) a_2 + ... + \alpha_{m-1}(\lambda_{m-1} - \lambda_m) a_{m-1} = 0$. Оскільки власні вектори $a_1, a_2, ..., a_{m-1}$ належать попарно різним власним значенням $\lambda_1, \lambda_2, ..., \lambda_{m-1}$, то, згідно з припущенням індукції, ці вектори лінійно незалежні, тобто з останньої рівності випливає, що $\alpha_1(\lambda_1 - \lambda_m) = \alpha_2(\lambda_2 - \lambda_m) = ... = \alpha_{m-1}(\lambda_{m-1} - \lambda_m) = 0$. Звідси отримуємо, $\alpha_1 = \alpha_2 = ... = \alpha_{m-1} = 0$, оскільки всі власні значення попарно різні. Тоді з рівності $\alpha_m a_m = 0$ отримуємо $\alpha_m = 0$, оскільки вектор a_m, як власний вектор, ненульовий. Отже, власні вектори $a_1, a_2, ..., a_m$ лінійно незалежні. Згідно з методом математичної індукції, теорема справедлива для довільного натурального *m*.

З теореми 1 випливає, що коли лінійний оператор *A* *n*-вимірного векторного простору *V* має *n* попарно різних власних значень, то власні вектори оператора *A*, що належать цим власним значенням, взяті по одному

для кожного значення, утворюють базис простору *V*. У базисі, складеному з власних векторів оператора *A*, матриця оператора *A* має надзвичайно простий вигляд, а саме, вона є діагональною, причому її діагональними елементами є власні значення, яким належать базисні вектори. Справді, якщо базисні вектори $e_1, e_2, ..., e_n$ є власними векторами оператора *A*, що належать власним значенням $\lambda_1, \lambda_2, ..., \lambda_n$ відповідно, то $Ae_1 = \lambda_1 e_1$, $Ae_2 = \lambda_2 e_2, ...,$ $Ae_n = \lambda_n e_n$, тому матриця оператора *A* в базисі $e_1, e_2, ..., e_n$ є діагональною матрицею:

$$A = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}.$$

Навпаки, якщо діагональна матриця *A* вказаного вище вигляду є матрицею оператора *A* в деякому базисі $e_1, e_2, ..., e_n$ векторного простору *V*, то $Ae_1 = [e_1] \cdot A = (1,0,...,0) \cdot A = (\lambda_1, 0,...,0) = \lambda_1 e_1$, $Ae_2 = [e_2] \cdot A = (0,1,0,...,0) \cdot A =$ $= (0, \lambda_2, 0,...,0) = \lambda_2 e_2, \ldots, Ae_n = [e_n] \cdot A = (0,...,0,1) \cdot A = (0,...,0, \lambda_n) = \lambda_n e_n$ тобто базисні вектори є власними векторами оператора *A*, що належать власним значенням $\lambda_1, \lambda_2, ..., \lambda_n$. Отже, справджується наступна теорема.

Теорема 2. Діагональна матриця $A = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$ є матрицею лінійного оператора *A* в деякому базисі векторного простору *V* тоді і тільки тоді, коли базисні вектори є власними векторами оператора *A*, що належать власним значенням $\lambda_1, \lambda_2, ..., \lambda_n$.

Лекція 18. Теорема про зв'язок характеристичних коренів матриці *A* та власних значень лінійного оператора *A*. Зведення матриць до діагонального виду

<u>Означення 1.</u> Рівняння виду

$$det\,(A-\lambda E)=0, \tag{1}$$

називається характеристичним рівнянням квадратної матриці *A*, його корені – характеристичними коренями матриці *A*.

Теорема 1. Для того, щоб скаляр λ_0 був власним значенням лінійного оператора *A*, необхідно і достатньо, щоб він був характеристичним коренем матриці лінійного оператора.

Необхідність. Нехай λ_0 – власне значення лінійного оператора *A*, тобто існує ненульовий вектор $\bar{x}_0$, що

$$A(\bar{x}_0)=\lambda_0\bar{x}_0 \tag{2}$$

Розглянемо матрицю $A=\{\alpha_{ik}\}^n$ лінійного оператора *A* в деякому базисі $B=\{\bar{b}_1,\ \bar{b}_2,\ \ldots,\ \bar{b}_n\}$. Якщо $\bar{x}_0=\sum_{k=1}^{n}\mu_k\bar{b}_k$, то підставляючи його значення в (2) отримаємо

$$\sum_{k=1}^{n}\mu_k A(\bar{b}_k)=\lambda_0\sum_{k=1}^{n}\mu_k\bar{b}_k \tag{3}$$

Підставимо в (3) $A(\bar{b}_k)=\sum_{i=1}^{n}\alpha_{ik}\bar{b}_i$ і прирівняємо відповідні коефіцієнти при $\bar{b}_i$ отримаємо

$$\sum_{k=1}^{n}\alpha_{ik}\mu_k=\lambda_0\mu_i,\quad i=\overline{1,n}, \tag{4}$$

тобто лінійну однорідну систему рівнянь відносно μ_i:

$$\sum_{\substack{k=1\\k\neq i}}^{n}\alpha_{ik}\mu_k+(\alpha_{ii}-\lambda_0)\mu_i=0,\quad i=\overline{1,n} \tag{5}$$

Визначником основної матриці системи (4) є $det\ (A-\lambda E)=0$. Оскільки система рівнянь (4) має ненульові розв'язки, то згідно наслідку теореми Крамера, $det\ (A-\lambda E)=0$, тобто λ_0 є характеристичним коренем матриці A.

Достатність. Якщо скаляр λ_0 є характеристичним коренем матриці A, то виконується рівність $det\ (A-\lambda E)=0$ і системи (5) має ненульовий розв'язок $(\mu_1, \mu_2, \ldots, \mu_n)$. Нехай $\bar{x}_0=\sum_{i=1}^{n}\mu_i\bar{b}_i$. Тоді, так як справджується (4), то й $\bar{x}_0$ задовільняє рівність (2). Теорема доведена.

<u>Означення 2.</u> Множина власних значень лінійного оператора називається його спектром.

<u>Означення 3.</u> Якщо всі n власних лінійного оператора дійсні і різні, то кажуть, що лінійний оператор має простий спектр.

Теорема 2. Якщо лінійний оператор a має простий спектр, то існує базис $B=\{\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n\}$, в якому матриця A лінійного оператора A є діагональною. При цьому базисом B є сукупність власних векторів, а діагональними елементами матриці A є відповідні власні значення.

Доведення. Нехай $\lambda_1, \lambda_2, \ldots, \lambda_n$ – дійсні різні власні значення лінійного оператора A. Тоді $A(\bar{b}_k)=\lambda_k\bar{b}_k,\ k=\overline{1,n}$

Як відомо, власні вектори, що відповідають попарно різним власним значенням є лінійно незалежні, а значить їх множина утворює базис $B=\{\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n\}$. Матрицею лінійного оператора A в цьому базисі B є

$$A=\begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ & & \ldots & \\ 0 & 0 & \ldots & \lambda_n \end{pmatrix}$$

Зауваження. Якщо лінійний оператор A не має простого спектра, але всі власні значення належать полю P (корені кратні), то вибором спеціального базису можна звести матрицю лінійного оператора A до нормальної форми Жордано, в якій відмінні від нуля елементи утворюють квадратні матриці, які розміщені вздовж діагоналі.

Лекція 19. Теорема про ділення з остачею в кільці цілих чисел. Найбільший спільний дільник та найменше спільне кратне двох чисел і зв'язок між ними. Алгоритм Евкліда

Теорема 1. Яке б не було ціле число a і натуральне число b, існує і притому єдина пара цілих чисел q і r така, що $a=bq+r$, причому $0\leq r<b$. Число q називають неповною часткою, а число r – остачею.

Доведення. Розглянемо послідовність всіх цілих чисел, які кратні b і розміщених в порядку зростання:

$\ldots (-2)b, (-1)b, a\cdot b, 1\cdot b, 2\cdot b, \ldots$

Так як ця послідовність є необмеженою як знизу, так і зверху, то існує таке ціле число q, що $b\cdot q\leq a< b(q+1)$. Віднімемо від цих частин одержаної нерівності $b\cdot q$, $0\leq a-bq<b$. Позначимо $a-bq$ через r, отримаємо $a=bq+r$, $0\leq r<q$.

Покажемо, що отримана пара чисел q, r – єдина. Припустимо від супротивного, що існує ще одна пара чисел q_1, r_1 таких, що $a=b\cdot q_1+r_1$, $0\leq r_1<b$. Тоді $b\cdot q_1+r_1= bq+r$ або $b(q-q_1)=r_1-r$.

Так як ліва частина ділиться націло на b, то й права частина ділиться націло на b, тобто $(r_1-r):b$. Це можливо лише тоді, коли $r_1-r=0$, тобто $r_1=r$. Якщо $r_1=r$, то $b\cdot q_1=b\cdot q$. Звідки слідує, що $q_1=q$. (При доведенні єдиності, ми скористалися такою модифікацією методу доведення від супротивного $a\Rightarrow b\equiv a\wedge\bar{b}\Rightarrow b$).

Теорема 2. Які б не були цілі числа a і $b\neq 0$, існує одна і тільки одна пара чисел q і r, така, що $a=bq+r$, $0\leq r</b/$

Доведення. Якщо $b>0$, то теорема 2 очевидна. Якщо $b<0$, то $b=-|b|$. Для пари чисел a, $|b|$, згідно теореми 1, існує єдина пара чисел q_1, r така, що $a=|b|\, q_1+r$, $0\leq r<|b|$. Звідси слідує, що $a=(-b)\cdot q_1+r$, або $a=b(-q_1)+r$. Позначивши – $q_1=q$, отримаємо $a=b\cdot q+r$.

Приклади.

1. $a=153;\ b=21$. Маємо $153=21\cdot 7+6;\ 0\le 6<7$

2. $a=-192,\ b=17$, маємо $-192=17(-12)+12,\ 0\le 12<17$

3. $a=-215,\ b=-19$, маємо $-215=(-19)\cdot 12+13,\ 0\le 12<|-19|$

З властивостей подільності цілого числа a на ціле число b випливає подільність $\pm a$ на $\pm b$, а тому можна обмежитися розглядом лише цілих додатніх чисел.

<u>Означення 1.</u> Ціле число d називається спільним дільником цілих чисел a і b, якщо кожне з цих чисел ділиться націло на d.

<u>Означення 2.</u> Найбільший із спільних дільників чисел a і b називається найбільшим спільним дільником цих чисел і позначається символом *НСД(a, b)*.

Теорема 3. Якщо цілі числа a,b,q,r пов'язані співвідношенням $a=bq+r$, то множина спільних дільників чисел a і b співпадає з множиною спільних дільників чисел b і r. Зокрема *НСД(a, b)=НСД(b, r)*.

Теорема 4. Найбільший спільний дільник чисел a і b дорівнює останній відмінний від нуля остачі r_n в алгоритмі Евкліда.

Доведення. Нехай a і b – натуральні числа. Якщо a не ділиться націло на b, то згідно теореми 1 існують такі цілі числа q_1, r_1, що $a=bq_1+r_1,\ 0<r_1<b$. Якщо b не ділиться націло на r_1, то згідно теореми 1 $b=r_1\ q_2+r_2,\ 0< r_2< r_1$. Якщо r_1 не ділиться націло на r_2, то $r_1=r_2\cdot q_3+r_3,\ 0<r_3<r_2$ і так дальше. Цей процес послідовного ділення не може продовжуватися нескінченно, бо в противному разі множина натуральних чисел $r_1> r_2> r_3>\ldots> r_{n-1}> r_n\ldots$ не матиме найменшого числа, що неможливо. Отже, існує таке n, що $r_{n-1}\vdots r_n$. процес послідовного ділення закінчиться через $n+1$ кроків і ми отримаємо таку систему рівностей:

$$a=bq_1+r_1$$

$$b= r_1q_2+r_2$$

$$r_1=r_2\cdot q_3+r_3$$

$$\ldots$$

$$r_{n-2}=r_{n-1}\cdot q_n+r_n$$

$$r_{n-1}=r_n\cdot q_{n+1}$$

Розглядаючи ці рівності зверху вниз, на підставі теореми 3 приходимо до висновку, що множина спільних дільників чисел a і b співпадає з множиною спільних дільників чисел b і r_1, з множиною спільних дільників чисел r_1 і r_2, r_2 і r_3 і т. д. з r_{n-1} і r_n, але $r_{n-1}:r_n$ значить $НСД(r_{n-1},r_n)=r_n$. Таким чином, ми отримали, що $НСД(a, b)=НСД(b, r_1)=НСД(r_1,r_2)=НСД(r_{n+1},r)=r$.

Приклад. $a=667$, $b=391$

$$\begin{array}{r|l}
667 & 391 \\ \cline{2-2}
-391 & 1 \\ \cline{1-1}
391 & 276=r_1 \\ \cline{2-2}
-276 & 1 \\ \cline{1-1}
276 & 115=r_2 \\ \cline{2-2}
-230 & 2 \\ \cline{1-1}
115 & 46=r_3 \\ \cline{2-2}
-92 & 2 \\ \cline{1-1}
46 & 23=r_4 \\ \cline{2-2}
-46 & 2 \\ \cline{1-1}
0=r_5 &
\end{array}$$

Отже, $НСД\ (667, 391)=23$.

<u>Означення 3.</u> Ціле число c, яке ділиться націло ціле число a та число b називається спільним кратним чисел a і b.

<u>Означення 4.</u> Найменше з додатніх спільних кратних чисел a і b називається найменшим спільним кратним цих чисел і позначається $НСК\ [a,b]$.

Теорема 5. Найменше спільне кратне натуральних чисел a і b дорівнює добутку цих чисел поділеному на їх найбільший спільний дільник, тобто $НСК[a,b]=\dfrac{a\cdot b}{НСД(a,b)}$.

Доведення. Нехай M – будь-яке спільне кратних двох чисел a і b. Так як $M:a$, то $M=a\cdot k$, де k – деяке ціле число. Але $M:b$, тому $\frac{M}{b}=\frac{a\cdot k}{b}\in Z$. Позначимо *НСД(a,b)* через d. Тоді $a=a_1d$ і $b=b_1d$, $\frac{M}{b}=\frac{a\cdot k}{b}=\frac{a_1dk}{b_1d}=\frac{a_1k}{b_1}$. Але $\frac{a_1k}{b_1}\in Z$ і a_1 та b_1 є взаємно простими, то $k:b_1$, тобто $k=b_1\cdot t=\frac{b}{2}$, де t- деяке ціле число. Таким чином, ми довели, що кожне спільне кратне M чисел a і b можна записати у виді $M=\frac{M}{b}=\frac{a\cdot b}{d}\cdot t$. Найменше спільне кратне чисел a і b отримаємо при $t=1$. Ми довели, що $НСК[a,b]=\frac{a\cdot b}{НСД(a,b)}$.

Приклад. Знайти *НСК[667, 391].*

Як відомо $НСК[667, 391]=\frac{667\cdot 391}{НСД(667,391)}=\frac{260797}{23}=11339$.

Вправи.

1. Довести теорему: якщо ціле число a ділиться націло на натуральне число b, то множина спільних дільників чисел a і b співпадає з множиною дільників числа b. Зокрема *НСД(a,b)=b.*

2. Як знаходити *НСД(a,b), НСК[a,b],* якщо відомі канонічні розклади чисел a, b?

3. Як знаходити *НСД* $(a_1, a_2, \dots, a_n)$?

4. Знайти *НСД(588,2058), НСД(299,391), НСК[279б372], НСК[667,299,391].*

Лекція 20. Прості числа. Нескінченність множини простих чисел. Основна теорема арифметики. Застосування канонічного розкладу чисел до знаходження *НСД(a,b), НСК[a,b]*

Відомо, що коли ціле число a ділиться націло на ціле число b, то $\pm a \vdots \pm b$, а тому будемо вивчати властивості цілих додатних чисел.

Означення 1. Натуральне число $p \neq 1$ називається простим числом, якщо воно має лише два дільники: 1 і p.

Означення 2. Натуральне число a називається складеним, якщо крім 1 і а воно має ще й інші дільники. Число 1 не належить ні до простих чисел, ні до складених чисел.

З означень 1, 2 випливають основні теореми про прості числа.

Теорема 1. Всяке натуральне число або ділиться націло на дане просте число р, або взаємно просте з p.

Теорема 2. Якщо добуток кількох натуральних чисел ділиться націло на просте число p, то принаймні один із співмножників ділиться націло на p.

Теорема 3. Найменший, відмінний від 1 дільник натурального числа a є просте число.

Теорема 4. Найменший, відмінний від 1 дільник складеного числа не більший від $\sqrt{a}$.

Теорема 5 (Евкліда). Множина простих чисел нескінченна.

Доведення. Припустимо, від супротивного, що множина простих чисел є скінченною і складається з простих чисел $p_1, p_2, \ldots, p_n$. Розглянемо число

$$p = p_1 \cdot p_2 \cdot \ldots \cdot p_{n+1}$$

Число p не співпадає ні з одним із чисел $p_1, p_2, \ldots, p_n$. Число p не може мати дільниками прості числа $p_1, p_2, \ldots, p_n$, бо інакше повинно ділитися націло на одне із чисел $p_1, p_2, \ldots, p_n$, що неможливо. Тому число p або саме є простим, що суперечить припущенню, або складеним. Якщо воно складене, то ділиться націло на просте число q, яке відмінне від простих чисел $p_1, p_2, \ldots, p_n$.

Звідси випливає, що існує ще одне просте число q, яке відмінне від $p_1, p_2, \ldots, p_n$, а це суперечить припущенню. Теорема доведена.

Теорема 6. (Основна теорема арифметики) Кожне відмінне від 1 натуральне число n можна представити у вигляді добутку простих чисел і притому єдиним способом, якщо не брати до уваги порядку розміщення співмножників.

Доведення. Нехай $n>1$ – будь-яке натуральне число. Згідно з властивістю простих чисел $n= p_1 n_1$, де p_1 – найменший простий дільник числа n. Якщо $n_1=1$, то $n=p_1$. Якщо $n_1>1$ і p_2 – найменший простий дільник числа n_1, то $n_1=p_2 \cdot n_2$, звідки $n=p_1 \cdot p_2 \cdot n_2$. Продовжуючи аналогічні міркування, отримаємо на деякому кроці, що $n_k=1$ (справді, числа $n_1, n_2, \ldots$ утворюють строго спадну послідовність натуральних чисел). Таким чином $n= p_1, p_2, \ldots, p_k$.

Доведемо єдиність такого розкладу. Припустимо, від супротивного, що існує ще один розклад натурального числа n в добуток простих множників $n=q_1 \cdot q_2 \cdot \ldots \cdot q_s$, а отже,

$$p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

Продовжимо аналогічні міркування. Після скінченного числа кроків отримаємо або $q_{k+1} \ldots q_s=1$, або $p_{s+1} \ldots p_k=1$, що неможливо, бо p_i і q_j є простими числами. Ми отримали, що $k=s$ та $p_1=q_1 \wedge p_2=q_2 \wedge \ldots \wedge p_k=q_s$.

Зауваження 1. При доведенні єдиності розкладу ми використали модифікацію доведення від супротивного $a \Rightarrow b \equiv a \wedge \bar{b} \Rightarrow b$.

Зауваження 2. В розкладі $n= p_1 \cdot p_2 \cdot \ldots \cdot p_k$ серед простих множників можуть бути і однакові. Якщо простий множник p_k повторюється в розкладі k раз, то його називають k- кратним множником числа n, або кажуть, що p_k має кратність k.

Позначимо через $p_1, p_2, \ldots, p_s$ різні множники в розкладі натурального числа n на прості множники, а $k_1, k_2, \ldots, k_s$ їхню кратність. Тоді $n = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$

<u>Означення 2.</u> Канонічним розкладом числа n на прості множники або канонічним зображенням числа n називається запис числа n у виді $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$

<u>Означення 3.</u> Факторизацією натурального числа n називається процес знаходження його канонічного розкладу.

Теорема 7. Якщо $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$ - канонічний розклад числа n, то всі дільники цього числа збігаються з числами виду $d = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_m^{s_m}$.

Теорема 8. Найбільший спільним дільником чисел a і b є число $НСД(a,b) = d = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_m^{l_m}$, де $a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_s}$ і $b = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_s^{m_s}$, $l_i = min(k_i, m_i)$, $i = 1, 2, \ldots, s$.

Доведення. Згідно теореми 7 всі спільні дільники чисел a і b збігаються з числами виду $d = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}$, $0 \le \alpha_i \le l_i$, $i = \overline{1, s}$. Серед усіх чисел такого виду найбільшим буде число, у якого показники α_i $(i = \overline{1, s})$ найбільші, тобто, число у якого $\alpha_i = l_s$. Отже, $НСД(a,b) = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_s^{l_s}$

Теорема 9. Найменшим спільним кратним чисел a і b є число

$$НСК[a,b] = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_s^{n_s},$$

де $n_i = max(k_i, m_i)$, $i = \overline{1, s}$

Доведення. Нехай M – будь-яке кратне чисел a і b. Число M ділиться на кожне з чисел a і b і тому воно ділиться на кожне з чисел $p_i^{n_i}$, де $n_i = max(k_i, m_i)$, $i = \overline{1, s}$. Оскільки для числа M існує тільки один канонічний розклад, то

$$M = p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_s^{t_s} \; p_1^{j_1} \cdot p_2^{j_2} \cdot q_r^{j_r},$$

де $t_i \ge n_i$, $j_\rho \ge 0$, $i = \overline{1, s}$, $\rho = \overline{1, r}$.

Серед усіх чисел такого виду найменшим буде те, у якого $t_i = n_i$, $j_\rho = 0$, $i = \overline{1, s}$, $\rho = \overline{1, r}$.

Лекція 21. Порівняння у кільці цілих чисел та їхні основні властивості. Повна та зведена система лишків. Т. Ейлера та Ферма

Розгляньмо пари цілих чисел виду $\langle a_i; m \rangle$, де a_i — будь-яке ціле число, m — фіксоване ціле додатне число. За теоремою про ділення з остачею, можемо записати: $a_i = mg_i + r_i$, де $g_i \in Z$, $0 \le r_i < m$, тобто $r_i \in \{0,1,2,...,m-1\}$. Оскільки цілих чисел нескінченна множина, а множина остач скінченна, то для певних різних чисел остачі, утворені при діленні a_i на m, повторюватимуться.

Введемо в множину цілих чисел Z нове бінарне відношення, що має місце при будь-якому фіксованому цілому додатному m.

Означення. Кажуть, число a перебуває у відношенні порівняння за модулем m з числом b, якщо остача від ділення числа a на m дорівнює остачі від ділення числа b на m.

Числа a і b, які перебувають у відношенні порівняння за модулем m, називають порівнюваними за даним модулем (або рівнолишковими) і записують $a \equiv b \pmod{m}$. Цей вираз називають порівнянням за модулем m.

Теорема (про рівносильні задання відношення порівняння). Порівнянність цілих чисел a і b за модулем m рівносильна:

1) можливості зображення числа a у вигляді $a = b + mg$, де $g \in Z$;
2) подільності $a - b$ на m.

Відношення порівняння за модулем m, задане у множині цілих чисел, має такі властивості.

I. Формальні властивості відношення порівняння.

Відношення порівняння за модулем має властивості рефлексивності, симетричності, транзитивності.

Доведення. $(\forall a \in Z)[m/a - a \Rightarrow a \equiv a(\bmod m)]$, тобто відношення порівняння рефлексивне.

$(\forall a \in Z)(\forall b \in Z)\left[a \equiv b(\bmod m) \Rightarrow m/a-b \Rightarrow m/_{b-a} \Rightarrow b \equiv a(\bmod m)\right]$, тобто відношення порівняння симетричне.

$(\forall a \in Z)(\forall b \in Z)(\forall c \in Z)$

$\left[a \equiv b(\bmod m) \wedge b \equiv c(\bmod m) \Rightarrow \ /m/_{a-b} \wedge m/_{b-c} \Rightarrow m/_{(a-b)+(b-c)} \Rightarrow m/_{a-c} \Rightarrow a \equiv c(\bmod m)\right]$,

тобто відношення порівняння транзитивне.

II. Властивості порівнянь за заданим модулем.

1. Порівняння за одним і тим самим модулем можна почленно додавати.

2. Порівняння за одним і тим самим модулем можна почленно перемножувати.

III. Властивості порівнянь, пов'язані із зміною модуля.

1. Обидві частини порівняння і модуль можна помножити на одне і те саме натуральне число.

2. Обидві частини порівняння і модуль можна скоротити на їхній спільний дільник.

3. Якщо порівняння виконується за модулем *m,* а число *d*—додатний дільник числа *m,* то воно виконується і за модулем *d*.

4. Якщо одна частина порівняння і модуль діляться на число *d,* то і друга частина порівняння ділиться на те саме число.

5. Якщо $a \equiv b(\bmod m)$, то *НСД (a; m) = НСД (b; m).*

Побудуймо алгебру з основною множиною $Z/_m$ ($Z/_m$- фактор-множина). Елементами цієї множини є класи, в кожний із яких потрапляють порівнянні між собою числа за модулем *m* і тільки вони, тобто числа, що дають при діленні на *m* однакову остачу. Оскільки різних остач при діленні на *m* рівно *m,* то і класів еквівалентності (тобто елементів множини $Z/_m$**)** рівно *m.* Клас еквівалентності, що містить деяке число *a,* позначатимемо $K_a^{(m)}$.

<u>Означення.</u> Фактор-множиною множини *A* за відношенням еквівалентності φ зветься таке розбиття множини *A* на класи, при якому будь-які два елементи, що належать одному і тому самому класу,

перебувають у відношенні φ, а елементи з різних класів не перебувають у цьому відношенні.

Згідно з означенням фактор-множини, клас $K_a^{(m)}$ дорівнює класу $K_b^{(m)}$ тоді і лише тоді, коли $a \equiv b \ (mod\ m)$.

<u>Означення 1.</u> Сумою класів $K_a^{(m)}$ і $K_b^{(m)}$ зветься клас, що містить елемент $a + b$, тобто $K_a^{(m)} \oplus K_b^{(m)} = K_{a+b}^{(m)}$.

<u>Означення 2.</u> Добутком класів $K_a^{(m)}$ і $K_b^{(m)}$ зветься клас, що містить елемент ab, тобто $K_a^{(m)} \otimes K_b^{(m)} = K_{ab}^{(m)}$.

<u>Означення 3.</u> Число a, що належить деякому класу множини Z/m, називають лишком цього класу.

<u>Означення 4.</u> Повною системою лишків за модулем m називають сукупність m цілих чисел, яка містить точно по одному елементу із кожного класу лишків за модулем m. Позначається $ПСЛ^{(m)}$.

<u>Означення 5.</u> Якщо із кожного класу лишків вибрати до $ПСЛ^{(m)}$ по найменшому невід'ємному лишку, то утворена сукупність m чисел матиме назву повної системи найменших невід'ємних лишків за модулем m. Позначається $ПСНЛ^{(m)}$.

Очевидно, що $ПСНЛ^{(m)} = \{0, 1, 2 \quad , m - 1\}$, оскільки m чисел даної множини являють собою остачі від ділення на m, а значить, всі ці числа потрапляють до різних класів, причому в своєму класі кожна із згаданих остач є найменшим невід'ємним лишком.

<u>Означення 6</u>. Якщо із кожного класу лишків вибрати до $ПСЛ^{(m)}$ найменший за абсолютною величиною лишок, то утворена сукупність m чисел називатиметься повною системою найменших абсолютних лишків. Позначається $ПСНАЛ^{(m)}$.

Для повної системи лишків за модулем m мають місце такі *властивості.*

1. Будь-яка сукупність m чисел $(m>1)$, попарно непорівнянних за модулем m, є повною системою лишків за модулем m.

Доведення. Нехай M — сукупність m чисел, попарно непорівнянних за модулем m. Тоді ці числа належать до різних класів лишків за модулем m. Крім того, M містить m чисел. Отже, множина M містить по одному представнику із кожного класу лишків за модулем m, тобто, за означенням, M являє собою $ПСЛ^{(m)}$.

2. Нехай $a \in Z$, $b \in Z$, $m \in \mathrm{N}$ і $НСД(a;m)=1$. Якщо x перебігає повну систему лишків за модулем m, то $ax+b$ теж перебігає повну систему лишків за цим модулем.

Доведення. Нехай M — повна система лишків за модулем m. Тоді множина $M_1 = \{ax + b / x \in M\}$, так само як і M, містить m елементів. Будь-які два числа $ax_i + b$ і $ax_j + b$ із M_1 непорівнянні, оскільки $x_i \not\equiv x_j \pmod{m}$. Отже, множина M_1, згідно з властивістю 1, є повною системою лишків за модулем m.

<u>Означення 7.</u> Числова функція, яка визначена на множині всіх цілих додатних чисел і для кожного конкретного цілого числа $m \neq 1$ дорівнює кількості чисел, що передують m і з ним взаємно прості, зветься функцією Ейлера. Позначають її $\varphi(m)$.

<u>Означення 8.</u> Зведеною системою лишків за модулем m називають сукупність цілих чисел, що містить по одному і тільки одному представнику із кожного класу лишків, взаємно простих з m. Позначають її $ЗвСЛ^{(m)}$.

Для зведеної системи лишків за модулем m мають місце такі *властивості.*

1. Будь-яка сукупність $\varphi(m)$ чисел $(m>1)$, взаємно простих з m і попарно непорівнянних за модулем m, є зведеною системою лишків за цим модулем.

2. Нехай $НСД(a;m)=1$. Якщо x пробігає зведену систему лишків за модулем m, то ax теж пробігає зведену систему лишків за цим модулем.

Теорема 3 (Ейлера). $(\forall a \in Z)(\forall m \in \mathrm{N})\left[(НСД(a,m)=1) \Rightarrow \left(a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)\right)\right]$.

Доведення. Нехай

$$a_1, a_2, ... a_{\varphi(m)} \qquad (1)$$

є зведена система лишків за модулем *m.* Тоді, за властивістю 2 зведеної системи лишків, сукупність чисел

$$aa_1, aa_2, ... aa_{\varphi(m)} \qquad (2)$$

так само є зведеною системою лишків за модулем *m.* Тому, за властивістю порівнянь добуток чисел сукупності (2) є порівнянним з добутком чисел сукупності (1) за модулем *m,* тобто

$$a^{\varphi(m)} \cdot a_1 \cdot a_2 \cdot ... \cdot a_{\varphi(m)} \equiv a_1 \cdot ... \cdot a_{\varphi(m)} (\mathrm{mod}\, m) \qquad (3)$$

Добуток $a_1 \cdot a_2 \cdot ... \cdot a_{\varphi(m)}$ — взаємно простий з *m,* тому (за властивістю відношення порівняння) обидві частини порівняння (3) можна поділити на цей добуток. Тоді $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$.

Теорема 4 (Ф е р м а) . $(\forall a \in \mathrm{Z})(\forall p \in \mathrm{N})[(p - \textit{просте}) \Rightarrow (a^{з-1} \equiv 1(\mathrm{mod}\, m))]$.

Д о в е д е н н я . Оскільки *p* — просте число, то всі числа *1, 2, p-1* з *p* взаємно прості, тобто *φ (p) = p-1*. Оскільки *НСД (a; p) = 1*, то, за теоремою Ейлера, маємо $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, p)$, тобто $a^{p-1} \equiv 1(\mathrm{mod}\, p)$.

Лекція 22. Лінійні порівняння з однією змінною. Теорема про число розв’язків. Метод розв’язування лінійних порівнянь

<u>Означення 1.</u> Порівняння виду

$$f(x) \equiv 0 (mod\ m), \qquad (1)$$

де $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$, x — довільне ціле число, $a_i \in Z$, $i = 0, 1, 2, \ldots n$, називається алгебраїчним порівнянням з однією змінною.

Якщо a_n не ділиться на число m, то число n називають степенем даного порівняння; якщо $a_n \vdots m$, то $a_n x^n \equiv 0 (\mathrm{mod}\, m)$, і тому в порівнянні його можна відкинути, в цьому випадку n не визначає степеня порівняння **(1).**

Нехай число a задовольняє порівняння **(1),** тобто перетворює його в правильне числове порівняння. Разом з числом a це порівняння задовольняють і всі числа класу лишків $K_a^{(m)}$ порівнянні з a за модулем m.

<u>Означення 2.</u> Р о з в ' я з к о м п о р і в н я н н я $f(x) \equiv 0 (mod\ m)$ називають клас лишків $K_a^{(m)}$, кожний лишок якого задовольняє це порівняння.

При такому означенні порівняння **(1)** матиме стільки розв'язків, скільки лишків $ПСЛ^{(m)}$ його задовольняють.

Оскільки $ПСЛ^{(m)}$ складається із m лишків, то порівняння **(1)** може мати тільки скінченну кількість розв'язків або не мати їх зовсім.

<u>Означення 3</u>. Алгебраїчне порівняння виду $a_1 x + a_0 \equiv 0\ (mod\ m)$ називається л і н і й н и м .

<u>Означення 4.</u> Лінійне порівняння

$$a_1 x + a_0 \equiv 0\ (mod\ m), \qquad (2)$$

де $a_1 \not\equiv 0\ (mod\ m)$, називають п о р і в н я н н я м п е р ш о г о с т е п е н я з о д н і є ю з м і н н о ю .

Порівняння **(2)** можна записати у вигляді $ax \equiv b\ (mod\ m)$.

<u>Означення 5.</u> Два порівняння називають р і в н о с и л ь н и м и , якщо множини чисел, що задовольняють ці порівняння збігаються.

Щоб побудувати порівняння, рівносильне заданому, над останнім виконують перетворення, які ґрунтуються на властивостях відношення порівняння.

Теорема (про кількість розв'язків порівнянь першого степеня з однією змінною). Нехай

$$ax \equiv b \pmod m \qquad (3)$$

— довільне порівняння першого степеня з однією змінною.

Якщо *НСД (a, m)*= 1, то порівняння (3) має єдиний розв'язок; якщо *НСД (a; m)= d (d >1)* і $d \,\bar{\vdots}\, b$, то порівняння (3) не має розв'язків; якщо *НСД (a; m) = d* і $d \vdots b$, то порівняння (3) має *d* розв'язків за модулем *m*.

Доведення. Частина I. Нехай *НСД (a; m) = 1*. Порівняння може мати не більше *m* розв'язків відповідно до кількості чисел у $ПСЛ^{(m)}$ Якщо *x* пробігає $ПСЛ^{(m)}$, то й вираз *ax-b* також пробігає $ПСЛ^{(m)}$. При цьому рівно один раз даний вираз набуде того числового значення, яке порівнянне з нулем, оскільки одним із лишків $ПСЛ^{(m)}$ є число із класу $K_0^{(m)}$. Нехай при *x = c* маємо *ac- b≡ 0 (mod m)*, тобто *ac = b (mod m)*. Тоді клас лишків $K_c^{(m)}$ і є єдиним розв'язком порівняння (3).

Частина II. Нехай *НСД (a; m) = d (d > 1)* і $d \vdots b$. Припустимо, що при деякому x_0 порівняння (3) задовольняється. Тоді $ax_0 \equiv b \pmod m$. Оскільки *НСД (a; m) = d*, то *НСД (b;m)=d*, що суперечить умові ($d \vdots b$). Тому припущення про існування розв'язку хибне.

Частина III. Нехай *НСД (a; m) = d (d > 1)* і $d \vdots b$. Записуємо: $a = a_x d$, $b = b_1 d$ $m = m_1 d$. Тоді, за властивістю відношення порівняння, одержимо порівняння

$$a_1 x \equiv b_1 \pmod{m_1}, \qquad (4)$$

яке рівносильне порівнянню (3). Оскільки НСД $(a_1, m_1)=1$, то останнє порівняння відповідно до частини I має єдиний розв'язок за модулем m_1, а саме $K_c^{(m_1)}$. Таким чином, порівняння (4) задовольняють числа виду $c + m_1 t$, де

$t \in Z$. Запишемо d таких чисел: $c, c + m_1, c+ 2m_1, \ldots, c+ (d- 1)m_1$. Всі ці числа порівнянні за модулем m_1 і непорівнянні за модулем m. Отже, за модулем m ці числа потрапляють до різних класів:

$$K_c^{(m)},\ K_{c+m_1}^{(m)}, \ldots,\ K_{c-(d-1)m_1}^{(m)}. \qquad (5)$$

Всі числа виду $c + m_1t$ потрапляють до одного із перелічених класів. Справді, нехай $s=c + m_1t$, де $t \in Z$. Ділимо t на d; дістаємо $t = dq +r$. Тоді $s = c + m_1dq+ m_1r= (c+ m_1r) + mq$, тобто $s = c +m_1r \ (mod\ m)$. Оскільки $r\in \{0, 1,\ldots, m-1\}$, то s належить до одного із класів сукупності (5). Таким чином, множина чисел, які задовольняють порівняння (3), складає один клас ($K_c^{(m_1)}$) за модулем m_1 і d класів ($K_c^{(m)},\ K_{c+m_1}^{(m)}, \ldots,\ K_{c-(d-1)m_1}^{(m)}$) за модулем m.

Із доведення теореми випливає, що для знаходження розв'язків порівняння першого степеня з однією змінною достатньо вміти знаходити розв'язок порівняння, коли a і m взаємно прості.

Існує багато способів розв'язування порівнянь такого виду. Називаємо основні.

<u>І спосіб.</u> Підстановка в порівняння чисел $ПСЛ^{(m)}$ (застосовується при невеликих модулях).

Приклад 1. Розв’язати порівняння: $2x \equiv 3(\mathrm{mod}7)$.

$ПСЛ(mod7)=\{0,1,2,3,4,5,6\}$. Так як $НСД(2, 7)=1$, то порівняння має єдиний розв’язок. Безпосередньою перевіркою переконуємося, що $x=5$ є розв’язком порівняння. Загальним розв’язком буде $x \equiv 5(\mathrm{mod}7)$ або $x \in K_{\mathrm{mod}7}^{(5)}$.

<u>ІІ спосіб</u>. Зведення порівняння першого степеня до рівносильного порівняння з коефіцієнтом при x, який дорівнює 1 (ґрунтується на проведенні низки рівносильних перетворень заданого порівняння на основі властивостей відношення порівняння).

Приклад 2. Розв’язати порівняння: $7x \equiv 8(\mathrm{mod}13)$. Так як $НСД(7, 13)=1$, то порівняння має єдиний розв’язок. Очевидно, що $0 \equiv 13(\mathrm{mod}13)$. Додамо почастинно ці порівняння: $7x \equiv 21(\mathrm{mod}13)$. Поділимо обидві частини порівняння на 7: $x \equiv 3(\mathrm{mod}13)$. Це і є розв’язок даного рівняння.

<u>III спосіб</u> (спосіб Ейлера). Нехай задано порівняння *ax* ≡ *b (mod m)*, де *НСД (a*; *m*) = *1*. Порівняння має єдиний розв'язок. За теоремою Ейлера, $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$. Правильним, очевидно, є і таке порівняння: $ba^{\varphi(m)} \equiv b(\mathrm{mod}\, m)$, або (що те саме)

$$a(a^{\varphi(m)-1}b) \equiv b(\mathrm{mod}\, m). \qquad (6)$$

Порівнюючи (6) з вихідним порівнянням, бачимо, що

$$x \equiv a^{\varphi(m)-1}b(\mathrm{mod}\, m) \qquad (7)$$

Приклад 3. Розв’язати порівняння: $5x \equiv 7(\mathrm{mod}13)$. Найбільший спільний дільник *НСД(5, 13)=1*. Порівняння має єдиний розв'язок. За формулою Ейлера $x \equiv 7 \cdot 5^{\varphi(13)-1}(\mathrm{mod}13)$. Так як 13- просте число, то $\varphi(13) = 12$. Маємо $x \equiv 7 \cdot 5^{11} = 7 \cdot (5^3)^3 \cdot 5^2 = 7 \cdot (125)^3 \cdot 25 \equiv 7 \cdot 12 \cdot 8^3 = 84 \cdot 64 \cdot 8 \equiv 6 \cdot 12 \cdot 8 = 48 \cdot 12 \equiv 9 \cdot 12 = 108 \equiv$ $\equiv 4(\mathrm{mod}13)$. Отже, $x \equiv 4(\mathrm{mod}13)$ - розв’язок даного порівняння.

Серед інших способів "розв'язування порівнянь зручним при великих модулях є спосіб, побудований на використанні скінченних ланцюгових дробів.

Додаткові запитання:

1. Як застосовується теорія порівнянь до розв’язування в цілих числах рівнянь $ax + by = c$?

2. Який алгоритм розв’язування систем порівнянь? Наприклад: $\begin{cases} x \equiv 3(\mathrm{mod}8) \\ x \equiv 11(\mathrm{mod}20) \\ x \equiv 1(\mathrm{mod}15) \end{cases}$.

Лекція 23. Застосування порівнянь до виведення ознак подільності

Будь-яке ціле число a можна зобразити у вигляді суми певних степенів основи g. Це дає змогу використати властивість відношення порівняння для виведення ознак подільності цілих чисел.

За властивістю подільності в кільці, маємо $m/a \Rightarrow \pm m/\pm a$. Тому достатньо вивести ознаки подільності натуральних чисел на натуральні. В цілому суть ознак подільності чисел зводиться до того, що розгляд питання про подільність натурального числа a на натуральне число m заміняється розглядом можливості подільності на число m іншого, меншого від a, натурального числа b_m, яке можна знайти за певним правилом, що визначається числовою функцією $f(a)$, тобто $b_m = f(a)$. При цьому числа a і $b_m = f(a)$ є, як кажуть, рівноподільними на число m, тобто такими, які одночасно діляться або одночасно не діляться на число m. Одним з методів знаходження ознак подільності, що ґрунтується на порівнянності чисел, є метод Паскаля, який будується на загальній ознаці подільності чисел (ознаці Паскаля).

Теорема (ознака Паскаля). Нехай $a = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g + a_0$ — систематичне зображення числа a у системі числення з основою g. Щоб довільне ціле число a ділилося без остачі на натуральне число m, необхідно і достатньо, щоб на m ділилося число

$$b_m = a_n r_n + a_{n-1} r_{n-1} + \ldots + a_1 r_1 + a_0, \qquad (1)$$

де $r_i \equiv g^i \pmod m$ $(i = 1, 2, \ldots, n)$.

Метод Паскаля для встановлення конкретних ознак подільності чисел полягає ось у чому.

а) Число a записують у десятковій системі числення у вигляді $a = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0$.

б) З порівнянь $10^i \equiv r_i \pmod m$ визначають r_i $(i = 1, 2, \ldots, n)$.

в) Будують вираз $b_m = a_n r_n + a_{n-1} r_{n-1} + \ldots + a_1 r_1 + a_0$.

г) Встановлюють специфіку визначення b_m через цифри числа a.

В результаті такого дослідження і ознаки Паскаля $(a \vdots m \Leftrightarrow b_m \vdots m)$ формулюють ознаку подільності на конкретне число *m*.

Послуговуючись цим методом, виведемо окремі ознаки.

***m* = 2** Оскільки $10^i \vdots 2$, $i \in \mathrm{N}$, то всі остачі r^i від ділення 10^i на число *2* дорівнюють нулю. Тому за формулою (1) число $b_2 = f(a) = a_0$. Отже, маємо таку ознаку: число *a* ділиться на *2* тоді і тільки тоді, коли на *2* ділиться цифра одиниць числа *a*.

***m* = 3** Остача від ділення *10* на *3* дорівнює *1*, тобто $10 \equiv 1 \pmod 3$. Тоді маємо: $10^i \equiv 1 \pmod 3$. Отже, $r_i = 1$ при будь-якому $i \in \mathrm{N}$. Тоді за формулою (1) $b_3 = f(a) = a_n + a_{n-1} 1 + \ldots + a_1 + a_0$. Маємо таку ознаку: число *a* ділиться на *3* тоді і тільки тоді, коли сума цифр, які його зображають, ділиться на *3*.

***m* = 11** За модулем 11, маємо $10^{2k} \equiv 1 \pmod{11}$, $10^{2k-1} \equiv 1 \pmod{11}$. Тому $r_{2k} = 1$, $r_{2k-1} = -1$. Отже, за формулою (1) $b_{11} = a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + \ldots =$ $= (a_0 + a_2 + a_4 + \ldots) - (a_1 + a_3 + a_5 + \ldots)$. Враховуючи, що цифри a_{2k} з парними індексами у числі b_{11} займають непарні місця, можна сформулювати таку ознаку: число *a* ділиться на *11* тоді і тільки тоді, коли різниця між сумою цифр, що займають непарні місця і сумою цифр, що займають парні місця, ділиться на *11*.

Ознаки подільності цінні, якщо вони прості, зручні для користування. Однак більшість ознак, які можна вивести на основі методу Паскаля, складні. Існує ряд ознак подільності, які не є наслідком загального методу Паскаля, а знайдені іншими шляхами.

Лекція 24. Перетворення звичайного дробу в десятковий та визначення довжини періоду десяткового дробу

Як відомо з арифметики звичайні дроби перетворюються в скінченні, або в нескінченні періодичні нескінченні дроби. При цьому звичайний дріб $\frac{a}{b}$ перетворюється в скінченний десятковий дріб тоді і тільки тоді, коли канонічний розклад знаменника має вигляд $2^{\alpha}5^{\beta}$, тобто не містить ніяких простих множників, крім 2 і 5. Для спрощення вважатимемо $\frac{a}{b}$ нескоротним правильним дробом. Звичайні нескоротні правильні дроби виду $\frac{a}{2^{\alpha}\cdot 5^{\beta}}$ перетворюється в скінченні десяткові дроби з числом десяткових знаків, яке дорівнює найбільшому з чисел α або β. Справді, якщо $\alpha=\beta$, то $\frac{a}{2^{\alpha}\cdot 5^{\beta}}=\frac{a}{2^{\alpha}\cdot 5^{\alpha}}=\frac{a}{10^{\alpha}}$ - скінченний десятковий дріб. Якщо $\alpha<\beta$, то $\frac{a}{2^{\alpha}\cdot 5^{\beta}}=\frac{a\cdot 2^{\beta-\alpha}}{2^{\beta}\cdot 5^{\beta}}=\frac{a\cdot 2^{\beta-\alpha}}{10^{\beta}}$ - скінченний десятковий дріб.

Якщо $\alpha>\beta$, то $\frac{a}{2^{\alpha}\cdot 5^{\beta}}=\frac{a\cdot 5^{\alpha-\beta}}{2^{\alpha}\cdot 5^{\alpha}}=\frac{a\cdot 5^{\alpha-\beta}}{10^{\alpha}}$ - скінченний десятковий дріб.

Нескоротний дріб виду $\frac{a}{c\cdot 2^{\alpha}\cdot 5^{\beta}}$ - де *c* відмінне від *2* і *5*, в скінченний десятковий дріб не перетворюється. Справді, припускаючи супротивне, маємо

$$\frac{a}{c\cdot 2^{\alpha}\cdot 5^{\beta}}=\frac{d}{10^{m}},$$

звідки $a\cdot 10^{m}=d\cdot c\cdot 2^{\alpha}\cdot 5^{\beta}$, де *c* - дільник числа $a\cdot 10^{m}$, що неможливо, бо *c* відмінне від *2* і *5* за умовою і *(a, c)=1*. Ця суперечність доводить справедливість твердження.

Теорема 1. Якщо канонічний розклад знаменника *b* нескоротного дробу $\frac{a}{b}$ не містить у собі множників *2* і *5*, то цей дріб перетворюється у

чистий періодичний десятковий дріб; при цьому число цифр у періоді дорівнює показнику δ, до якого належить число *10*, за модулем *b*.

Доведення. Для спрощення дріб $\frac{a}{b}$ вважатимемо правильним. Процес ділення числа *a* на число *b* при умові *a* < *b* можна подати у вигляді системи рівностей:

$$\begin{aligned} 10a &= bq_1 + r_1, \\ 10r_1 &= bq_2 + r_2, \\ &\ldots\ldots\ldots\ldots \\ 10r_{m-1} &= bq_m + r_m, \\ 10r_m &= bq_{m+1} + r_{m+1}, \\ &\ldots\ldots\ldots\ldots\ldots \end{aligned} \qquad (1)$$

де $r_1, r_2, ..., r_m, r_{m+1}, ...$ — остачі, а $q_1, q_2, ..., q_m, q_{m+1}, ...$ — частки проміжних обчислень. Будь-яка остача r_i очевидно, задовольняє нерівність

$0 < r_i < b,$ а будь-які числа q_i задовольняють нерівність $0 \le q_i < 10,$ тобто є цифрами, з яких складається частка $0, q_1, q_2, ..., q_m, q_{m+1}, ...$ Проаналізуємо властивості чисел r_i і q_i докладніше. Насамперед нагадаємо, що дріб $\frac{a}{b}$ є нескоротним і правильним. Це означає, що *(a,b)=1* і $a < b$. Таким чином, число *a* є один з найменших додатних лишків ЗСЛ за модулем *b*.

Покажемо тепер, що й усі r_i також є найменшими додатними лишками ЗСЛ за модулем *b*. Справді

$$[(a,\ b) = 1 \wedge (10, b) = 1)] => [(10a, b) = 1]. \qquad (2)$$

Оскільки числа *10a* і *b* взаємно прості, то з першої рівності (1) випливає, що $(r_1, b) = 1$. Справді з умови $(r_1, b) = d > 1$ випливало б, що вся права частина, а отже, і ліва частина ділилась би на *d*. Тому числа *10a* і *b* не були б взаємно простими, що суперечить (2). З умов $0 < r_i < b,\ (r_1, b) = 1$ випливає, що остача r_1 є одним з найменших додатних лишків ЗСЛ за модулем *b*. Аналогічно можна показати, що й числа $r_2, ..., r_m, r_{m+1}, ...$ є найменшими

додатними лишками ЗСЛ за модулем *b*. Але ЗСЛ за модулем *b* може мати не більше $\varphi(b)$ найменших додатних лишків. Тому в системі рівностей (1) настане момент, коли одна з остач дорівнюватиме *a*. Нехай $r_m = a$. Тоді $m + 1$ рівність (1) збіжиться з першою рівністю цієї системи. І тому $q_1 = q_{m+1}$, $r_1 = r_{m+1}$. Далі, $m + 2$ -а рівність збіжиться з другою рівністю (1) і тому $q_2 = q_{m+2}$, $r_2 = r_{m+2}$. Таким чином, остачі r_i і частки q_i- проміжних обчислень повторюватимуться. Тим самим частка буде чистим періодичним десятковим дробом виду

$$0,(q_1, q_2, ..., q_m). \qquad (3)$$

Для доведення теореми залишається показати, що перше повторення настане після δ кроків проміжних обчислень, де δ — показник, до якого належить *10* за модулем *b*. Справді, якщо δ — найменший показник, при якому здійснюється конгруенція

$$10^{\delta} \equiv 1(\mathrm{mod}\, b),$$

то при $r < b$ і $(r, b) = 1$ рівносильною їй є і конгруенція

$$10^{\delta} \cdot r \equiv r(\mathrm{mod}\, b).$$

Остання конгруенція якраз і показує, що, приписавши до r δ нулів, що відповідає визначенню δ послідовних цифр частки, дістанемо при діленні $10^{\delta} \cdot r$ на *b* остачу *r*. При діленні *a* на *b* при $(a, b)=1$ і $a<b$ аналогічно дістанемо через δ ділень остачу, яка дорівнює числу *a*. Отже, частка (3) має вигляд $0,(q_1, q_2, ..., q_{\delta})$, що й треба було довести.

Зауваження. З конгруенції $10^{\delta} \equiv 1(\mathrm{mod}\, b)$ випливає, що $10^{\delta} - 1 \equiv 0(\mathrm{mod}\, b)$, або $\underbrace{999...9}_{\delta\text{цифр}} \equiv 0(\mathrm{mod b})$.

Іншими словами, число 999...9, що складається з δ дев'яток,— найменше з можливих чисел такої структури, яке ділиться на *b*. Це дає можливість досить легко знаходити число δ. Для цього треба послідовно ділити на *b* числа 9, 99, 999, 9999, ... і т. д., аж поки таке ділення не відбудеться. Кількість дев'яток у такому числі і дорівнює числу δ.

Теорема 2. Якщо канонічний розклад знаменника b нескоротного дробу $\frac{a}{b}$ має вигляд $b = 2^{\alpha} \cdot 5^{\beta} \cdot c$, де *(c, 10) = 1*, то цей дріб перетворюється у мішаний періодичний дріб; число цифр до періоду дорівнює γ, де γ — найбільше з чисел α і β - число цифр періоду дорівнює δ, де δ — показник, якому належить число *10* за модулем c.

Доведення. Дріб $\frac{a}{b} = \frac{a}{2^{\alpha} \cdot 5^{\beta} \cdot c}$ помножимо на 10^{λ}, де $\gamma = \max\{\alpha, \beta\}$.

Матимемо $\frac{10^{\gamma} \cdot a}{b} = \frac{a \cdot 2^{\gamma-\alpha} \cdot 5^{\gamma-\beta}}{c} = \frac{a_1}{c}$

і далі $[(a,b)=1 \wedge (2,c)=1 \wedge (5,c)=1] \Rightarrow [(a \cdot 2^{\gamma-\alpha} \cdot 5^{\gamma-\beta}, c)=1] \Rightarrow [(a_1, c)=1]$.

За теоремою 1, дріб $\frac{a_1}{c}$ перетворюється в чистий періодичний дріб з числом цифр у періоді, яке дорівнює δ, де δ — показник, до якого належить *10* за модулем *c*. Щоб з нього дістати початковий дріб $\frac{a}{b}$, треба розділити його на 10^{γ}, або інакше, перенести кому в знайденому періодичному дробі на γ знаків ліворуч; у результаті дістанемо мішаний періодичний дріб з числом γ цифр до періоду. Теорему доведено.

Лекція 25. Многочлени над полем. Теорема про ділення з остачею. *НСД* двох многочленів. Алгоритм Евкліда

З курсу математичного аналізу відомо, що многочленом від однієї змінної є ціла раціональна функція виду

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \qquad (1)$$

задана на всій дійсній осі, де коефіцієнти a_n, a_{n-1}, …, a_1, a_0 —довільні задані дійсні числа.

Вимагатимемо, щоб кільце R *не мало дільників нуля,* тобто щоб

$$a, b=0 \Leftrightarrow a=0 \vee b=0$$

для довільних $a, b \in R$ (0 — нульовий елемент кільця).

Комутативне кільце, в якому не існує дільників нуля, називається областю цілісності. Отже, вважатимемо, що коефіцієнти многочленів, які ми розглядаємо, належать деякій області цілісності R.

<u>Означення 1.</u> *Многочленом* (поліномом) *від однієї змінної над областю цілісності R* називається вираз виду

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \qquad (2)$$

де n — довільне ціле невід'ємне число, a_n, a_{n-1}, …, a_1, a_0 — елементи R, а x (або x^1), x^2, ..., x^{n-1}, x^n - деякі символи; x^k називається *k-м степенем змінної x* (або невідомого *x),* а a_k — *k-м коефіцієнтом многочлена* (2) або *коефіцієнтом при* x^k $(k = 0, 1, ..., n)$.

Многочлени від змінної x позначаються маленькими латинськими буквами: $f(x)$, $g(x)$, $q(x)$, $s(x)$ і т. п., сукупність усіх многочленів від x над областю цілісності R символом $R[x]$.

<u>Означення 2.</u> Вираз $a_k x^k$ $(k = 1, ..., n-1, n)$ називається *k-м членом або членом k-го степеня многочлена*

$$f(x)= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \qquad (3)$$

a_0 - нульовим або вільним членом, причому записи a_0 *і* a_0x^0 рівнозначні. Якщо $a_к=0$ (тобто є нульовим елементом області цілісності R), то кажуть, що *k-й* член многочлена $f(x)$ дорівнює нулю або його немає.

Відповідно до означень 1 і 2 різні члени многочлена від однієї змінної є завжди членами різних степенів. Зауважимо, що *k-й* коефіцієнт $a_к$ многочлена іноді називають коефіцієнтом його *k*-го члена.

<u>Означення 3.</u> Відмінний від нуля член многочлена $f(x)$, степінь якого більший за степінь усіх інших відмінних від нуля членів цього многочлена, називається *старшим членом,* його коефіцієнт — *старшим коефіцієнтом,* а його степінь — *степенем многочлена* $f(x)$.

Степінь многочлена $f(x)$ позначають $deg\ f$.

Дії над многочленами

Нехай дано два многочлени над областю цілісності *R*.

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, (a_i \in R,\ i = 0, 1, \ldots, n), \quad (4)$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0, (b_j \in R,\ j = 0, 1, \ldots, m). \quad (5)$$

Означимо спочатку поняття рівності многочленів (4) і (5).

<u>Означення 4.</u> Многочлени $f(x)$ і $g(x)$ називають *рівними* між собою і записують $f(x) = g(x)$, якщо канонічні форми цих многочленів збігаються, тобто

$$[f(x) = g(x)] \underset{df}{\equiv} [n = m] \wedge \bigwedge_{k=0}^{n} [a_k = b_k]. \quad (6)$$

З означення 1 безпосередньо випливає, що рівність многочленів має властивості рефлексивності, симетричності та транзитивності, тобто є відношенням еквівалентності на множині $R[x]$.

Означимо тепер суму многочленів (4) і (5). Без обмеження загальності можна вважати, що $n \geq m \geq 0$.

<u>Означення 5.</u> *Сумою многочленів* $f(x)$ і $g(x)$ називається многочлен

$$s(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_{m-1}x^{m-1} + (a_m + b_m)x^m + (a_{m-1} + b_{m-1})x^{m-1} + \ldots +$$
$$+ (a_1 + b_1)x + (a_0 + b_0), \quad (7)$$

Те, що $s(x)$ є сумою многочленів $f(x)$ і $g(x)$, записують так:

$$s(x) = f(x) + g(x).$$

З цього означення випливають важливі наслідки:

Наслідок 1. Якщо $f(x)\ R \in [x]$, $g(x)\ R \in [x]$, то й $f(x) + g(x) \in R[x]$. Справді,

для коефіцієнтів d_k многочлена $f(x) + g(x)$ маємо з (7):

$$\begin{cases} a_k, k = n, n-1, ..., m+1, \\ a_k + b_k, k = m, m-1, ..., 1, 0. \end{cases} \quad (8)$$

Наслідок 2. Степінь суми двох многочленів не перевищує більшого з степенів даних многочленів: $deg\ (f + g) \leq max\ \{deg\ f, deg\ g\}$.

Наслідок 3. Для довільного многочлена $f(x)\ R \in [x],\ \theta(x)\ R \in [x]$

$$f(x) + g(x) = f(x). \quad (9)$$

<u>Означення 6.</u> Добутком многочленів $f(x)$ і $g(x)$ називається многочлен

$$p(x) \underset{df}{=} c_{n+m} x^{n+m} + c_{n+m-1} x^{n+m-1} + \ldots + c_1 x + c_0, \quad (10)$$

де $c^k \underset{df}{=} \sum_{j=0}^{k} a_{k-j} b_j = a_k b_0 + a_{k-1} b_1 + \ldots + a_1 b_{k-1} + a_0 b_k\ (k = 0, 1, \ldots, n+m)$,

$$a_{k-j} = 0 \text{ при } k-j > n,\ b_i = 0 \text{ при } j > m. \quad (11)$$

Те, що $p(x)$ є добуток многочленів $f(x)$ і $g(x)$, записують так: $p(x)=f(x)g(x)$.

Наслідок 4. Якщо $f(x)\ R \in [x],\ g(x)\ R \in [x]$, то й $f(x)\ g(x) \in R\ [x]$.

Наслідок 5. Якщо $f(x)$ і $g(x)$ не є *нуль-многочлени, то*

$$deg\ (f\ g) = deg\ f + deg\ g. \quad (12)$$

Нехай R- область цілісності, $R[x]$ — сукупність усіх многочленів над R.

Існують властивості сукупності $R[x]$ многочленів над областю цілісності R, які не залежать від специфічних особливостей R, а лише від того, що R є областю цілісності. Саме такі спільні для усіх $R[x]$ властивості розглянемо.

Теорема 1. Сукупність $R[x]$ усіх многочленів над областю цілісності R є область цілісності відносно операцій додавання та множення многочленів.

Справедливе твердження: $R[x]$ є кільце з одиницею тоді і тільки тоді, коли R є кільце з одиницею.

Вимагатимемо, щоб область цілісності R була полем, тобто щоб в R для довільного елемента $a \neq 0$ існував обернений елемент a^{-1}, або щоб

$$\underset{a,b \in R}{\forall} [a \neq 0 \Rightarrow \underset{c \in R}{\exists} [c = a^{-1} b \underset{df}{=} \frac{b}{a}]].$$

Сукупність усіх многочленів над полем P є область цілісності з одиницею $P[x]$ відносно додавання і множення многочленів.

Особливо важливу роль в елементарній алгебрі, в аналізі та теорії функцій, а також у практичних застосуваннях математики відіграють многочлени над числовими полями, тобто многочлени над полем C комплексних чисел або його підполями (R, Q та ін.). Оскільки числові поля мають характеристику нуль, для многочленів над числовими полями алгебраїчне означення многочлена рівносильне функціональному. Це полегшує вивчення їх і дає змогу встановити ряд важливих спеціальних властивостей.

Теорема 2. Довільний многочлен $f(x)$ з кільця $P[x]$ ділиться з остачею на будь-який многочлен $g(x)$ з цього кільця, відмінний від нуль - многочлена; при цьому частка й остача також належать до $P[x]$ і визначаються однозначно.

Доведення. Встановимо спочатку саму можливість знайти серед многочленів з кільця $P[x]$ частку $s(x)$ і остачу $r(x)$ для будь-яких многочленів $f(x), g(x) \in P[x]$ при $g(x) \neq 0$. Нехай

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0.$$

Якщо $f(x)=0$, то зрозуміло, що $s(x)=0$, $r(x)=0$.

Нехай тепер $n = \deg f < \deg g = m$; тоді можна вважати, що $s(x) = 0$, $r(x)=f(x)$. Залишається розглянути випадок, коли $n \geq m$. Виконаємо доведення методом індукції по n, починаючи з $n = 0$. При $n = 0$ маємо $m = 0$, $f(x) = a_0$, $g(x)=b_0 \neq 0$, тому $s(x) = \frac{a_0}{b_0}$, а $r(x) = 0$. Очевидно, $s(x) \in P[x]$, бо $\frac{a_0}{b_0} \in P$.

Припустимо, що теорема справедлива для всіх многочленів таких, що $\deg f < n$, і доведемо її для многочленів степеня n.

Розглянемо многочлен

$$p(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$

(a_n і b_m відмінні від нуля). Старший член многочлена $\frac{a_n}{b_m}x^{n-m}g(x)$ (який належить $P[x]$) дорівнює $a_n x^n$, тобто старшому члену многочлена $f(x)$. Тому $\deg p < n$, і за припущенням індукції $p(x)$ можна поділити з остачею на $g(x)$:

$$p(x) = g(x)\, s_1(x) + r_1(x);\ s_1(x),\ r_1(x) \in P[x];$$

$$r_1(x) = 0 \text{ або } \deg r_1 < \deg g.$$

Отже,

$$f(x) - \frac{a_n}{b_m}x^{n-m}g(x) = g(x)\, s_1(x) + r_1(x),$$

звідки $f(x) = g(x)\, s(x) + r(x)$, де

$$r(x) = r_1(x),\ s(x) = s_1(x) + \frac{a_n}{b_m}x^{n-m}.$$

Звідси $s(x)$ і $r(x)$ належать $P[x]$ і що $r(x)=0$ або $\deg r = \deg r_1 < \deg g$. Цим показано можливість ділення $f(x)$ на $g(x)$ з остачею.

Щоб закінчити доведення теореми, слід встановити єдиність частки $s(x)$ і остачі $r(x)$. Припустимо, що можливі два записи:

$$f(x) = g(x)\, s(x) + r(x),\ \deg r < \deg g;$$

$$f(x) = g(x)\, \hat{s}(x) + \hat{r}(x),\ \deg \hat{r} < \deg \hat{g}.$$

Віднімаючи другу рівність від першої, дістанемо

$$g(x)[s(x) - \hat{s}(x)] = r(x) - \hat{r}(x). \qquad (13)$$

За умовою $g(x) \neq 0$. Якщо припустити, що $r(x) \neq \hat{r}(x)$, то й $s(x) \neq \hat{s}(x)$ (адже кільце $P[x]$ не має дільників нуля). Але тоді ми приходимо до суперечності. Справді, права частина (13) є многочлен, степінь якого менший від $\deg g$ і, отже, менший від степеня лівої частини рівності $f(x)=g(x)s(x)+r(x)$. Отже, рівність (13) можлива лише при $r(x) = \hat{r}(x)$ і $s(x) = \hat{s}(x)$, що й свідчить про єдиність частки і остачі. Теорему доведено.

Як наслідок з попереднього викладу дістаємо таке важливе твердження:

Теорема 3. Кільце $P[x]$ многочленів над полем P є евклідове кільце.

Теорема 4 (Безу). Для будь-якого елемента α з поля P остача при

діленні многочлена $f(x) \in P[x]$ на $x - \alpha$ дорівнює $f(\alpha)$.

<u>Означення 7.</u> Якщо многочлен $d(x)$ є дільником многочлена $f(x)$ і многочлена $g(x)$, то він називається *спільним дільником многочленів* $f(x)$ і $g(x)$.

<u>Означення 8.</u> Спільний дільник многочленів $f(x)$ *і* $g(x)$, який ділиться на кожний інший спільний дільник цих многочленів, називається *найбільшим спільним дільником многочленів* $f(x)$ і $g(x)$ і позначається через (f, g).

Ці означення природно узагальнюються на випадок m $(m>2)$ многочленів.

Звичайно, будь-які два многочлени мають тривіальні спільні дільники, а саме — дільники одиниці кільця $P[x]$; такими дільниками є усі відмінні від нуля константи (елементи поля P). Очевидно також, що НСД двох многочленів не визначається цілком однозначно. Якщо $d(x)$ — найбільший спільний дільник, то й кожний многочлен $cd(x)$, де c — елемент поля P, відмінний від нуля, також є НСД цих многочленів. Проте *з точністю до сталого множника найбільший спільний дільник визначається однозначно.* Справді, якщо $d(x)$ і $d_1(x)$ — найбільші спільні дільники даних двох многочленів, то $d(x)$ повинен ділитися на $d_1(x)$, а $d_1(x)$ повинен ділитися на $d(x)$. Тоді $d(x)$ і $d_1(x)$ асоційовані, тобто $d_1(x) = cd(x)$, де с — константа, відмінна від нуля.

<u>Означення 9.</u> *Спільним кратним многочленів* $f(x)$, $g(x) \in P[x]$ називається будь-який многочлен $s(x) \in P[x]$ такий, що $s(x) \vdots f(x) \wedge s(x) \vdots g(x)$. *Найменшим спільним кратним (НСК) многочленів* $f(x), g(x)$ називається спільне кратне $f(x)$ і $g(x)$, яке ділить будь-яке інше спільне кратне цих многочленів; НСК многочленів $f(x)$ і $g(x)$ позначають $[f, g]$.

Теорема 5. Для будь-яких відмінних від нуля многочленів $f(x)$, $g(x)$ найменше спільне кратне існує і визначається однозначно з точністю до сталого множника.

Розглянемо спосіб знаходження найбільшого спільного дільника двох многочленів.

Оскільки $P[x]$ є евклідове кільце, у ньому застосовна процедура знаходження *НСД* за допомогою послідовного ділення з остачею або алгоритму Евкліда. Тут ми розглянемо **алгоритм Евкліда** стосовно до знаходження *НСД* двох многочленів.

Нехай дано два многочлени $f(x)$ і $g(x)$, причому степінь $f(x)$ не менший від степеня $g(x)$. Виконаємо послідовне ділення з остачею, яке можна записати за допомогою такої системи рівностей:

$$
\begin{gathered}
f(x) = g(x)s_1(x) + r_1(x), \\
g(x) = r_1(x)s_2(x) + r_2(x), \\
r_1(x) = r_2(x)s_3(x) + r_3(x), \\
\ldots\ldots\ldots\ldots\ldots\ldots \\
r_{n-2}(x) = r_{n-1}(x)s_n(x) + r_n(x), \\
r_{n-1}(x) = r_n(x)s_{n+1}(x).
\end{gathered}
\tag{14}
$$

Ми тут виходимо з того, що після скінченного числа ділень остача $r_{n+1}(x)$ дорівнюватиме *0*. Справді, з самого означення остачі зрозуміло, що степінь многочлена $r_1(x)$ менший від степеня $g(x)$; степінь $g_2(x)$ менший від степеня $g_1(x)$ і взагалі степінь $r_k(x)$ менший від степеня $r_{k-1}(x)$. Але це означає, що або якась з остач $r_k(x)$ дорівнюватиме нулю, або степінь остачі, зменшуючись при кожному діленні принаймні на одиницю, дорівнюватиме нулю. Якщо $\deg r_n = 0$, то $r_{n+1}(x) = 0$, бо будь-який многочлен ділиться на многочлен нульового степеня. У всякому разі алгоритм Евкліда для многочленів зводиться до скінченного числа ділень з остачею. Оскільки степінь $r_1(x)$ не більший за *m-1* , де *m*– степінь $g(x)$, то число кроків у схемі (14) не може перевищувати *m*.

Відповідно до загальної теорії остання відмінна від нуль-многочлена остача у системі рівностей (14) і є НСД многочленів $f(x)$ і $g(x)$.

Приклад. Знайти найбільший спільний дільник многочленів $P(x) = x^3 - x^2 + x - 1$, $Q(x) = x^2 + (1+i)x + i$.

Застосуємо алгоритм Евкліда:

$$
\begin{array}{r|l}
x^3 - x^2 + x - 1 & x^2 + (1+i)x + i \\ \cline{2-2}
\underline{x^3 + (1+i)x^2 + ix} & x - (2+i) \\
- \quad -(2+i)x^2 + (1+i)x - 1 & \\
\underline{-(2+i)x^2 - (3i+1)x - (2i-1)} & \\
(2-2i)x - (2-2i) & \vdots\ (2-2i)
\end{array}
$$

$$
\begin{array}{r|l}
- \quad x^2 + (1+i)x + i & (x-1) \\ \cline{2-2}
\underline{x^2 - x} & x + (2+i) \\
-(2+i)x + i & \\
\underline{(2+i)x - (2+i)} & \\
2 + 2i & \vdots\ (2-2i)
\end{array}
$$

$$
\begin{array}{r|l}
- \quad x - 1 & 1 \\ \cline{2-2}
\underline{x - 1} & x - 1 \\
0 &
\end{array}
$$

Лекція 26. Факторіальність кільця. Факторіальність кільця многочленів над полем

Нижче використовуються наступні позначення: *К*- факторіальне кільце, *F* — поле елементів кільця *К*; *К[x]* — кільце многочленів від *x* над *К*; *F[x]* — кільце многочленів від x над *F*.

<u>Означення 1.</u> Нехай $f = a_0 + a_1 x + ... + a_n x^n$ — довільний ненульовий многочлен з *К[x]*. Найбільший спільний дільник коефіцієнтів $a_0, a_1, ..., a_n$ в кільці *К* називається змістом многочлена *f*.

<u>Означення 2.</u> Многочлен *f*, складовою якого є одиниця або дільник одиниці (у *К*), називається примітивним в кільці *К [x]*.

Зміст многочлена *f* у *К[x]* визначається однозначно з точністю до множників, що є дільниками одиниці. Іншими словами, будь-які дві складові многочлена *f* асоційовані в *К*.

Теорема. Якщо *d* — складова ненульового многочлена з *К[x]*, то *f = dg*, де *g* — примітивний в *К[x]* многочлен.

Відмітимо, що всякий многочлен, який незвідний над кільцем *К* додатнього степеня примітивний в *К[x]*. Дійсно, якщо *f* непримітивний, то за теоремою *f = dg*, де *g* — примітивний в *К[x]* многочлен додатнього степеня, а *d* — елемент *f*. Оскільки *f* непримітивний, то *d* не є дільником одиниці в *К* і, значить, *d* і *g* — необоротні елементи *К[x]*. Отже *f* приводимо в *К[x]*. Таким чином, всякий непримітивний многочлен додатнього степеня звідний в *К[x]*, а, отже, всякий незвідний в *К[x]* многочлен додатнього степеня примітивний в *К[x]*.

Відмітимо також, що примітивний в *К[x]* многочлен звідний над *К* тоді і тільки тоді, коли його можна представити у вигляді добутку многочленів додатнього степеня (причому примітивних). Для довільного непримітивного многочлена *f* це невірно, оскільки можливо, що *f = dg*, де *d* — елемент *f* і *deg d = 0*, а *g* — примітивний незвідний многочлен.

Лема 1. Нехай *f, h* — примітивні в *К[x]* многочленів і

$$cf = dh, \qquad (1)$$

де $c, d \in K\backslash\{0\}$.

Тоді d асоційований із c в K і f асоційований з h в $K[x]$.

Лема 2. Нехай f і h — примітивні в $K[x]$ многочлени. Якщо многочлени f і h асоційовані в $F[x]$, то вони асоційовані також в $K[x]$.

Лема 3 (Гаусса). Добуток примітивних в $K[x]$ многочленів є примітивним в $K[x]$ многочленом.

Лема 4. Нехай f — многочлен в $K[x]$. Якщо многочлен f звідний в $F[x]$, то він звідний також в $K[x]$.

Теорема. Якщо кільце K факторіальне, то і кільце многочленів $K[x]$ факторіальне.

Доведення. Нехай K — факторіальне кільце. Доведемо, що будь-який відмінний від нуля необоротний елемент кільця $K[x]$ однозначно з точністю до порядку співмножників і оборотних множників розкладемо в добуток простих множників в $K[x]$. Спочатку доведемо можливість розкладання на прості множники. Нехай f — довільний ненульовий многочлен з К[x]. Якщо f — многочлен нульового степеня, то $f \in K$. Оскільки кільце K факторіальне, многочлен f можна представити у вигляді добутку простих множників в K і, значить, в $K[x]$. Припустимо, що $deg\ f = n > 0$, і всякий многочлен, степінь якого менше n, розкладемо в добуток простих множників. Нехай

$$f = dg(x), \qquad (2)$$

де $d \in K$, $g(x)$ — многочлен додатнього степеня, примітивний в $K[x]$. Якщо многочлен g незвідний над K, то, розкладаючи в (2) множник d на прості множники, отримаємо розкладання f на прості множники. Якщо ж многочлен $g(x)$ звідний в $K[x]$, то його можна представити у вигляді добутку двох многочленів додатнього степеня, меншого, ніж n: $g(x)=h(x)\varphi(x)$. По індуктивному припущенню, $h(x)$ і $\varphi(x)$ можна представити у вигляді добутку простих множників в $K[x]$. Отже, g, а в силу (2) і f також можна представити у вигляді добутку простих множників.

Доведемо єдиність розкладання. Нехай дано будь-які два розкладання f

на прості множники в $K[x]$:

$$f=p_1 \dots p_k q_1 \dots q_s = p_1' \dots p_r' q_1' \dots q_t', \quad (3)$$

де p_i, $p_i' \in K$, і q_i, q_i' - незвідні, а значить, і примітивні многочлени додатнього степеня. Із лем 1 і 3 з (3) випливає, що

$$p_1 \dots p_k \sim p_1' \dots p_r' \text{ в } K \quad (4)$$

$$q_1 \dots q_s \sim q_1' \dots q_t' \text{ в } K[x]. \quad (5)$$

Оскільки кільце K факторіальне, то з (4) слідує, що $k=r$

$$p_i \sim p_i' \text{ в } K \text{ для } i = 1 \dots k. \quad (6)$$

Многочлени q_i і q_i' незвідні в кільці $F[x]$. В силу факторіальності кільця $F[x]$ з (5) випливає, що $s = t$:

$$q_i \sim q_i' \text{ в } F[x] \text{ для } i = 1, \dots, s.$$

Многочлени q_i і q_i' - незвідні в $K[x]$ і, значить, примітивні в $K[x]$, крім того, ці многочлени асоційовані в $F[x]$. Отже, по лемі 2, вони асоційовані в $K[x]$.

$$q_i \sim q_i' \text{ в } K[x] \text{ для } i = 1, \dots, s. \quad (7)$$

В силу (6) і (7) поліном f володіє однозначним розкладанням на прості множники в кільці $K[x]$. Отже, показано, що кільце $K[x]$ факторіальне.

Додаткові запитання:

1. Звідний чи незвідний многочлен x^2+2x+2: (a) у кільці $Q[x]$; (b) у кільці $R[x]$?

2. Всякий незвідний у кільці $Z[x]$ поліном є примітивним в $Z[x]$. Чи вірне обернене твердження?

Лекція 27. Алгебраїчна замкненість поля комплексних чисел. Канонічний розклад многочленна над полем комплексних чисел та його єдність

Нехай нам дано рівняння виду $f(x) = 0$, де $f(x)$ — довільний многочлен з однією змінною над полем комплексних чисел.

Кожний многочлен є функцією від аргументу x. Якщо $x_i \in C$, то функціональні значення ($f(x_i)$) многочлена теж комплексні числа. Такі функції називають <u>комплексними функціями комплексної змінної</u>. Кожному аргументу x_i відповідає функціональне значення многочлена $f(x_0)$, а йому відповідає $|f(x_0)|$. Таким чином, $|f(x)|$ також є функцією від аргументу x. Назва цієї функції — <u>модуль многочлена</u> $f(x)$. Тут аргумент $x \in C$, а всі значення функції $|f(x)|$ є дійсними числами. Такі функції звуться <u>дійсними функціями комплексної змінної.</u>

Основними *властивостями* функції $|f(x)|$, де $f(x) \in C[x]$, $x \in C$ є:

<u>Властивість 1.</u> $|f(x)|$ - функція неперервна.

<u>Властивість 2.</u>

$$(\forall f(x) \in C[x])(\forall n \in N)(\forall \varepsilon \in R_+)(\exists \delta \in R_+)(\forall x \in C)$$

$$\left[f(x) = a_n x^n + \ldots + a_1 x \Rightarrow \left(|x| < \delta \Rightarrow |f(x) < \varepsilon|\right)\right]$$

<u>Властивість 3.</u> $(\forall f(x) \in C[x])(\forall n \in N)(\forall m \in R_+)(\exists r_0 \in R_+)(\forall x \in C)$, $\left[|x| > r_0 \Rightarrow |f(x) > m|\right]$, де n - степінь многочлена $f(x)$.

<u>Властивість 4.</u>

$(\forall f(x) \in C[x])(\forall n \in N)(\forall x_0 \in C)(\exists h \in C \setminus \{0\})\left[f(x) \neq 0 \Rightarrow \left|f(x_0 + h) < |f(x_0)|\right|\right]$, де n - степінь многочлена $f(x)$. (Лема Д'Аламбера).

<u>Властивість 5.</u> $(\forall f(x) \in P[x])(\forall x \in C)(\exists x_0 \in C)\left[|f(x_0)| \leq |f(x)|\right]$.

Теорема 1 (теорема Гаусса). Кожний многочлен з $C[x]$ степеня $n \geq 1$ має у C хоча б один корінь.

Доведення. Нехай x_0 — комплексне число, яке задовольняє властивість 5 функції $|f(x)|$, тобто $|f(x_0)| \le |f(x)|$ на всій множині комплексних чисел. Доведімо, що $f(x_0) = 0$.

Припустімо супротивне. Нехай $f(x_0) \neq 0$. Тоді, за властивістю 4 функції $|f(x)|$ знайдеться таке комплексне число h, що $\left[\left| f(x_0 + h) < |f(x_0)| \right|\right]$, яке суперечить вибору x_0. Отже, $f(x_0) = 0$, тобто x_0 — корінь многочлена $f(x)$. Теорему Гаусса називають *основною теоремою про існування кореня.*

Наслідки з теореми Гаусса

I. Незвідними над полем C є тільки многочлени першого степеня.

Доведення. Многочлен першого - степеня незвідний над будь-яким числовим полем, у тому числі і над C. Будь-який многочлен $f(x)$ з $C[x]$ степеня $n \ge 2$ завжди звідний над C. Справді, за теоремою Гаусса, у C існує хоча б один корінь x_0 многочлена $f(x)$. Тоді, $f(x) = (x - x_0)\, g(x)$, де $g(x)$ — многочлен степеня $n - 1$ з кільця $C[x]$. Звідси випливає, що $f(x)$ звідний над C.

II. Будь-який многочлен $f(x) = a_n x^n + \ldots + a_1 x + a_0$ (степеня $n \ge 1$) з кільця $C[x]$ має над C єдиний канонічний розклад на незвідні нормовані множники:

$$f(x) = a_n (x - \alpha_1)^{k_1} \cdot (x - \alpha_2)^{k_2} \cdot \ldots \cdot (x - \alpha_s)^{k_s}.$$

Доведення. $f(x) = cp_1^{k_1}(x) \cdot cp_2^{k_2}(x) \cdot \ldots \cdot cp_s^{k_s}(x)$, причому цей розклад визначається однозначно з точністю до числового множника c і порядку слідування множників.

Оскільки (за наслідком I) незвідними над C є лише многочлени першого степеня, то канонічний розклад многочлена $f(x)$ над C має вигляд $f(x) = c(a_1 x + b_1)^{k_1} \cdot (a_2 x + b_2)^{k_2} \cdot \ldots \cdot (a_s x + b_s)^{k_s}$.

Виносячи a_i $(i = 1, 2, \ldots, n)$ за дужки і позначаючи $-\dfrac{b_i}{a_i} = \alpha_i$, $ca_1^{k_1} a_2^{k_2} \cdot \ldots \cdot a_s^{k_s} = d$, маємо $f(x) = d(x - \alpha_1)^{k_1} \cdot (x - \alpha_2)^{k_2} \cdot \ldots \cdot (x - \alpha_s)^{k_s}$.

Виходячи з означення алгебраїчної рівності многочленів, прирівнюємо старші коефіцієнти многочленів, що знаходяться у лівій і правій частинах рівності, дістаємо при цьому єдине значення *d*: $d = a_n$. Отже,

$$f(x) = a_n(x-\alpha_1)^{k_1} \cdot (x-\alpha_2)^{k_2} \cdot \ldots \cdot (x-\alpha_s)^{k_s}$$

Теорема 2 . Поле *C* алгебраїчно замкнене.

Доведення. Для доведення цієї теореми досить показати, що всі корені всіх многочленів із кільця *C[x]* належать множині *C*.

За наслідком II з теореми Гаусса, для будь-якого многочлена $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ степеня $n \geq 1$ з кільця *C[x]* маємо

$$f(x) = a_n(x-\alpha_1)^{k_1} \cdot (x-\alpha_2)^{k_2} \cdot \ldots \cdot (x-\alpha_s)^{k_s}. \qquad (1)$$

Звідси випливає, що $\alpha_1 \in C$ є k_1- кратним коренем многочлена *f(x),* $\alpha_2 \in C$ — k_2 - кратний корінь многочлена *f(x)* і т. д.

З рівності (1) доходимо висновку, що $n = k_1 + k_2 + \ldots + k_s$, тобто многочлен *f(x)* має у *C n* коренів, рахуючи кожний корінь стільки разів, яка його кратність. За теоремою про найбільшу кількість коренів многочлена з урахуванням їхньої кратності, більше за *n* коренів многочлен *f(x)* мати не може. Отже, всі *n* коренів многочлена *f(x)* належать *C*.

Таким чином, доведенням теореми про алгебраїчну замкненість поля *C* завершується розв'язання проблеми про розв'язність рівнянь виду *f(x) = 0*, де *f(x)* — довільний многочлен степеня $n \geq 1$ з коефіцієнтами з довільної числової області цілісності.

Лекція 28. Многочлени з дійсними коефіцієнтами. Спряженість уявних коренів таких многочленів. Незвідні над полем дійсних чисел многочлени та канонічний розклад многочленів над полем дійсних чисел

Рівняння з дійсними коефіцієнтами є поширеним і важливим для практичних застосувань окремим випадком алгебраїчних рівнянь з комплексними коефіцієнтами. Оскільки дійсні числа утворюють підполе поля K комплексних чисел, то будь-який многочлен n-го степеня з дійсними коефіцієнтами має точно n комплексних коренів.

Але в багатьох випадках особливий інтерес становлять саме дійсні корені рівнянь з дійсними коефіцієнтами. Ми знаємо, що рівняння з дійсними коефіцієнтами може взагалі не мати жодного дійсного кореня (наприклад, рівняння $x^2 + 1 = 0$). Проте виявляється, що основна теорема алгебри дозволяє зробити ряд висновків і щодо коренів рівнянь з дійсними коефіцієнтами.

Теорема 1. Якщо комплексне число z_0 є коренем многочлена з дійсними коефіцієнтами

$$P(z)= a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0, \qquad (1)$$

то спряжене комплексне число $\bar{z}_0$ також є коренем цього многочлена.

Доведення. Обчислимо значення $P(z_0)$. Відокремивши дійсну і уявну частини, матимемо:

$$P(z_0)= a_n z_0^n + a_{n-1} z_0^{n-1} + \ldots + a_1 z_0 + a_0 = A + Bi. \qquad (2)$$

Але z_0 є коренем многочлена (1), тому $A + B_i = 0$, звідки $A=B= 0$. Обчислимо тепер вираз $P(\bar{z}_0)$. Через те що всі коефіцієнти a_k — дійсні числа, то $\bar{a}_k = a_k$ і тому

$$P(\bar{z}_0)=a_n(\bar{z}_0)^n + a_{n-1} (\bar{z}_0)^{n-1} + \ldots + a_1 \bar{z}_0 + a_0 = \bar{a}_n (\bar{z}_0)^n + \bar{a}_{n-1} (\bar{z}_0)^{n-1} + \ldots +$$

$$+ \bar{a}_n \bar{z}_0 + \bar{a}_0 \qquad (3)$$

Порівнюючи (2) і (3), бачимо, що $P(\bar{z}_0)$ можна дістати з $P(z_0)$ в результаті заміни всіх чисел спряженими. Оскільки над цими числами виконуються лише дії додавання і множення, тому $P(z_0)$ і $P(\bar{z}_0)$ є спряжені комплексні числа, тобто $P(\bar{z}_0) = \overline{[P(z_0)]} = A - B_i$. Але ми вже показали, що $A=B=0$. Отже, $P(\bar{z}_0)=0$, і тому $\bar{z}_0$ є коренем даного рівняння. Теорему доведено.

Цю теорему природно доповнити таким твердженням.

Теорема 2. Якщо комплексне число z_0 є коренем k-ої кратності ($k>1$) многочлена $P(z)$ з дійсними коефіцієнтами, то спряжене комплексне число $\bar{z}_0$ є коренем многочлена $P(z)$ тієї ж кратності k.

Доведення. Оскільки z_0 є коренем $P(z)$ кратності k, то

$$P(z_0) = P'(z_0) = \ldots = P^{(k-1)}(z_0);\ P^{(k)}(z_0) \neq 0. \qquad (4)$$

Але всі похідні від $P(z)$ мають також дійсні коефіцієнти. Тому, застосовуючи теорему 1 до многочленів $P^{(j)}(z)$ можемо зробити, висновок що $P^{(j)}(\bar{z}_0)=0$ $(j=1, 2, .,. , k-1)$. З другого боку, $P^{(k)}(\bar{z}_0)\neq 0$, бо в протилежному випадку за теоремою 1 число z_0, спряжене з $\bar{z}_0$, також було б коренем $P^{(k)}(z)$, що суперечить (4). Отже,

$$P(\bar{z}_0) = P'(\bar{z}_0) = \ldots = P^{(k-1)}(\bar{z}_0);\ P^{(k)}(\bar{z}_0) \neq 0.$$

Це й означає, що z_0 є коренем, многочлена $P(z)$ кратності k.

Теорема 3. Кожний многочлен $P(z)$ над полем дійсних чисел допускає єдиний розклад на незвідні множники в цьому полі виду:

$$P(z) = a_n(z-z_1)^{k_1}\cdot(z-z_2)^{k_2}\cdot\ldots\cdot(z-z_l)^{k_l}\cdot(z^2+p_{l+1}z+q_{l+1})^{k_l+1}\ldots(z^2+p_m z+q_m)^{k_m}. \qquad (5)$$

Доведення. Для $P(z)$ у йолі дійсних чисел можливий розклад виду

$$P(z) = [P_1(z)]^{k_1}\cdot\ldots\cdot[P_m(z)]^{k_m} \qquad (6)$$

причому $P_1(z), \ldots, P_m(z)$ — незвідні у полі D многочлени, які визначаються з точністю до сталого множника. Якщо поставити вимогу, щоб старші коефіцієнти цих многочленів дорівнювали 1, то вони визначатимуться

однозначно. $P_k(z)$ є многочленами не вище 2-го степеня. Припустимо, що $P_1(z)$, … ,$P_l(z)$ є множники 1-го степеня, а $P_{l+1}(z)$, …,$P_m(z)$ — незвідні множники 2-го степеня (може трапитись, що $l=0$ або $l=m$). Тоді (6) матиме вигляд:

$$P(z) = A(z-\alpha_1)^{k_1} \cdot (z-\alpha_2)^{k_2} \cdot \ldots \cdot (z-\alpha_l)^{k_l} \cdot (z^2 + p_{l+1}z + q_{l+1})^{k_l+1} \ldots (z^2 + p_m z + q_m)^{k_m}$$

A дорівнює старшому коефіцієнту многочлена a_n, а $-\alpha_1$, $-\alpha_2$, … , $-\alpha_l$ - його дійсні корені z_1, z_2, …., z_l; отже, цей розклад збігається з (5), і теорему доведено.

Теорема 3 показує, що розклад многочлена $P(z)$ в полі дійсних чисел на незвідні множники дозволяє знайти всі його корені (бо степінь незвідних множників не перевищує 2). Проте в загальному випадку, щоб знайти цей розклад, треба в свою чергу знайти корені даного многочлена. Задача знаходження коренів многочлена по суті рівносильна задачі розкладання многочлена на незвідні множники в полі D.

Лекція 29. Многочлени над полем раціональних чисел. Цілі і раціональні корені многочленна з цілими коефіцієнтами. Незвідні над полем раціональних чисел многочлени

Наявність раціональних коренів у довільно взятого алгебраїчного рівняння — явище досить рідкісне. Тому знаходження таких коренів не має великого практичного значення. Але, якщо многочлен $f(x)$ над полем Q раціональних чисел, або, що те саме, рівняння

$$f(x)= a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 =0$$

з раціональними коефіцієнтами має раціональні корені, то в багатьох випадках ці корені можна знайти за допомогою цілком елементарних способів. Знаючи навіть один корінь r, можна спростити дане рівняння, звівши його до рівняння $(n - 1)$-го степеня діленням на $x - r$.

У зв'язку з цим доцільно ознайомитися з елементарними способами знаходження раціональних коренів многочленів з кільця $Q[x]$. Знання цих прийомів особливо важливе для вчителя математики, оскільки в практиці шкільного викладання алгебраїчні рівняння, як правило, зустрічаються з раціональними коефіцієнтами і досить часто з раціональними коренями. Тому знання специфічних властивостей многочленів з раціональними коефіцієнтами потрібне вчителю для вибору доцільного методу розв'язування конкретних рівнянь у шкільному курсі.

Основна відмінність многочленів над полем Q раціональних чисел від многочленів над полем R всіх дійсних чисел або полем C всіх комплексних чисел полягає в тому, що існують многочлени з раціональними коефіцієнтами як завгодно високого степеня, незвідні у полі раціональних чисел, тоді як у кільці $C[x]$ звідним є довільний многочлен, степінь якого вищий від одиниці, а в кільці $R[x]$ звідним є кожний многочлен, степінь якого перевищує 2, навіть якщо цей многочлен не має жодного дійсного кореня. Перш ніж доводити існування незвідних многочленів будь-якого степеня в полі Q, розглянемо деякі властивості многочленів з раціональними

коефіцієнтами.

Насамперед зауважимо, що будь-яке алгебраїчне рівняння з раціональними коефіцієнтами множенням на спільний знаменник усіх коефіцієнтів можна звести до рівняння з цілими коефіцієнтами.

Оскільки зручніше мати справу з цілими, а не з дробовими числами, ми далі намагатимемося зводити всі питання щодо многочленів над полем Q до відповідних питань відносно многочленів з цілими коефіцієнтами. Зокрема, так можна зробити з питанням про звідність многочлена в полі Q. Для цього нагадаємо спочатку означення примітивного многочлена відносно кільця Z.

<u>Означення 1.</u> Многочлен $p(x)$ з цілими коефіцієнтами називається примітивним, якщо його коефіцієнти не мають спільних дільників, відмінних від ± 1.

Лема. Добуток двох примітивних многочленів є примітивним многочленом.

Розглянемо тепер питання про звідність многочлена з цілими коефіцієнтами в полі раціональних чисел.

Теорема 1. Для того щоб многочлен $f(x)$ з цілими коефіцієнтами був звідним у полі Q, раціональних чисел, необхідно і достатньо, щоб він був звідним у кільці Z цілих чисел, тобто щоб існували многочлени $f_1(x)$ і $f_2(x)$ ненульового степеня з цілими коефіцієнтами такі, що $f(x)= f_1(x)\, f_2\,(x)$.

Доведення. Необхідність. Нехай дано многочлен з цілими коефіцієнтами $f(x)$, звідний у полі раціональних чисел, тобто $f(x)= g_1(x)g_2(x)$, де $g_1(x)$, $g_2(x)$ — многочлени ненульового степеня з раціональними коефіцієнтами. Потрібно довести, що існують многочлени ненульового степеня $f_1(x)$ і $f_2(x)$ з цілими коефіцієнтами, добуток яких дорівнює $f(x)$.

Нехай після зведення коефіцієнтів до спільного знаменника і винесення цього знаменника за дужки многочлен $g_1(x)$ має вигляд: $g_1(x)=\dfrac{\alpha}{\beta}s_1(x)$, де $s_1(x)$ — многочлен з цілими коефіцієнтами, β — спільний знаменник коефіцієнтів $g_1(x)$, а α — найбільший спільний дільник коефіцієнтів

многочлена, що утворюється з $g_1(x)$ після зведення до спільного знаменника. Зрозуміло, що $s_1(x)$ є примітивний многочлен. Можна вважати, що $(\alpha,\beta)=1$, бо інакше можна було б виконати скорочення. Аналогічно, для $g_2(x)$ маємо: $g_2(x)=\frac{\gamma}{\delta}s_2(x)$, де $s_2(x)$ — примітивний многочлен, а $(\gamma,\delta)=1$. Отже,

$$f(x)=\frac{\alpha\gamma}{\beta\delta}\cdot s_1(x)\cdot s_2(x).$$

Доведемо, що $\frac{\alpha\gamma}{\beta\delta}$ - дорівнює цілому числу. Справді, припустимо,

Що $\frac{\alpha\gamma}{\beta\delta}=\frac{p}{q}$, де p і q — взаємно прості числа. Добуток $s_1(x)\cdot s_2(x)=s(x)$ за лемою є примітивний многочлен. Нехай c_k — якийсь коефіцієнт $s(x)$. Добуток $\frac{p}{q}c_k$ має бути цілим числом при будь-якому k, бо $f(x)=\frac{p}{q}s(x)$ має цілі коефіцієнти. Але p взаємно просте з q, тому c_k має ділитися на q. Оскільки те саме повинно справджуватись для всіх коефіцієнтів c_k, дістаємо суперечність з тим, що $s(x)$ примітивний многочлен. Отже, $\frac{\alpha\gamma}{\beta\delta}=m$, де m — ціле число. Узявши $f_1(x)=ms_1(x)$, $f_2(x)=s_2(x)$, дістанемо $f(x)=f_1(x)f_2(x)$, де $f_1(x)$, $f_2(x)$ — многочлени ненульового степеня з цілими коефіцієнтами.

Достатність. Якщо $f(x)$ звідний у кільці цілих чисел, то він і тим більше звідний у полі раціональних чисел, бо кожний многочлен з цілими коефіцієнтами є многочленом над полем раціональних чисел. Теорему доведено.

Теорема 2 (Ейзенштейна). Якщо в многочлені з цілими коефіцієнтами

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$$

коефіцієнти $a_0, a_1, \ldots, a_{n-1}$ діляться на деяке просте число p, причому a_0 не ділиться на p^2, а старший коефіцієнт a_n не ділиться на p, то многочлен $f(x)$ незвідний у полі раціональних чисел.

Доведення. Згідно з теоремою 1, досить показати, що $f(x)$ при цих умовах не може бути добутком двох многочленів ненульового степеня з цілими коефіцієнтами. Припустимо супротивне, тобто що

$$f(x)= (b_r x^r + b_{r-1} x^{r-1} + ... + b_1 x + b_0)(c_s x^s + c_{s-1} x^{s-1} + ... + c_1 x + c_0)\ (r+s=n).$$

Вважатимемо для конкретності, що $r \geq s$. Маємо:

$$\begin{aligned} a_0 &= b_0 c_0, \\ a_1 &= b_1 c_0 + b_0 c_1, \\ a_2 &= b_2 c_0 + b_1 c_1 + b_0 c_2, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ a_r &= b_r c_0 + b_{r-1} c_1 + ... + b_{r-s} c_s, \\ a_n &= b_r c_s. \end{aligned} \qquad (1)$$

За умовою, a_0, тобто $b_0 c_0$, повинно ділитися на p, але не може ділитися на p^2. Отже, на p ділиться лише одне з чисел: b_0 або c_0. Нехай, наприклад, b_0 ділиться на p, а c_0 не ділиться. Але тоді з другої рівності системи (1) дістаємо, що b_1 ділиться на p (бо a_1 ділиться на p за умовою, а c_0 не ділиться). Тепер уже b_0 і b_1 діляться на p, тому з третьої рівності видно, що й b_2 ділиться на p. Так можна показати, що всі коефіцієнти b_0, b_1 , b_2, ..., b_{r-1} і b_r ділиться на p. Але це неможливо, бо тоді й a_n ділилося б на p (це випливає з останньої рівності (1)), що суперечить умові теореми. Теорему доведено.

За допомогою теореми 2, яку часто називають критерієм Ейзенштейна, можна розв'язати питання про незвідність у полі раціональних чисел ряду многочленів з кільця $Q[x]$.

Проте основне значення теореми 2 полягає в тому, що з неї випливає *існування многочленів довільного степеня з цілими коефіцієнтами, незвідних у полі раціональних чисел.* Зокрема, при всякому натуральному n і простому p многочлен $f(x) = x^n + p$ напевне незвідний у полі Q. Зрозуміло, що такі многочлени можна побудувати багатьма способами.

Теорема 3. У кільці многочленів над полем раціональних чисел є многочлени довільного степеня, незвідні у полі Q.

Теорема 2 дає достатню умову незвідності многочлена в полі Q. Легко дати і достатню умову звідності многочлена у полі Q, а саме:

Теорема 4. Якщо многочлен $f(x)$ з раціональними коефіцієнтами,

степінь якого більший за одиницю, має хоча б один раціональний корінь r, то $f(x)$ звідний у полі раціональних чисел.

Теорема 5. Якщо многочлен третього степеня $f(x)$ з раціональними коефіцієнтами не має раціональних коренів, то він незвідний у полі раціональних чисел.

Доведення. Припустимо супротивне. Нехай $f(x) = f_1(x)\, f_2(x)$, де $f_1(x)$ і $f_2(x)$ — многочлени ненульового степеня з кільця $Q[x]$. Оскільки сума степенів $f_1(x)$ і $f_2(x)$ дорівнює 3, то один з цих многочленів обов'язково має степінь 1, а другий — степінь 2. Нехай $f_1(x)$ є многочленом 1-го степеня з раціональними коефіцієнтами $f_1(x) = ax + b$. Але тоді число $x_0 = -\frac{b}{a}$ є раціональним коренем многочлена $f_1(x)$, а тому й многочлена $f(x)$. Виходить, що $f(x)$ має раціональні корені, що суперечить умові. Теорему доведено.

Теорема 6. Для того щоб $\frac{p}{q}$, де $(p,q)=1$, було раціональним, коренем многочлена з цілими коефіцієнтами

$$f(x)= a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

необхідно, щоб при довільному цілому k число $f(k)$ ділилося на $p-qk$ (якщо тільки $p-qk \neq 0$).

Доведення. Поділимо $f(x)$ на $x - k$. Маємо

$$f(x) = (x-k)(b_{n-1} x^{n-1} + \ldots + b_1 x + b_0) + f(k). \quad (2)$$

Усі коефіцієнти частки $b_{n-1}, \ldots, b_1, b_0$ є цілими числами. Підставляючи в (2) $x = \frac{p}{q}$ і враховуючи, що $f(\frac{p}{q})=0$, матимемо:

$$-f(k) = \left(\frac{p}{q} - k\right)\left[b_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + b_1\left(\frac{p}{q}\right) + b_0\right].$$

Помноживши обидві частини на q^n, дістанемо

$$-q^n f(k) = (p-qk)\left[b_{n-1}p^{n-1} + \ldots + b_1 pq^{n-2} + b_0 q^{n-1}\right],$$

звідки видно, що $q^n f(k)$ ділиться на $p-qk$, якщо $p-qk \neq 0$.

Покажемо тепер, що q і $p-qk$ взаємно прості. Справді, якби вони мали

спільний дільник $\alpha, |\alpha| \neq 1$, то і $p=qk+(p-qk)$ мало б цей дільник, що неможливо, бо $(p, q)= 1$. Отже, q і $p-qk$, а тому і q^n і $p-qk$ взаємно прості. Через те що добуток $q^n f(k)$ ділиться на $p-qk$, то це означає, що $f(k)$ ділиться на $p-qk$. Теорему доведено.

Наслідок. Якщо старший коефіцієнт a_n даного многочлена $f(x)$ з цілими коефіцієнтами дорівнює одиниці, то його раціональними коренями можуть бути лише такі цілі числа p, для яких $f(k)$ ділиться на p-k при всякому цілому k, при якому $p-k \neq 0$.

Теорема 6 дає змогу дістати довільну кількість необхідних умов того, щоб число $\frac{p}{q}$ було коренем даного рівняння, бо числу k можна надавати довільних цілих значень. Найбільш поширені на практиці умови, що відповідають $k=\pm 1$, бо вирази $f(1)$ і $f(-1)$ легко обчислити, їх можна сформулювати так: Щоб число — було раціональним коренем многочлена з цілими коефіцієнтами, треба щоб $\frac{f(1)}{p-q}$ і $\frac{f(-1)}{p-q}$ були цілими числами.

Зауважимо, що замість того, щоб підставляти раціональне число r у многочлен $f(x)$, можна поділити $f(x)$ на x-r. Якщо остача дорівнюватиме нулю, то r буде коренем $f(x)$, у противному разі r не буде коренем $f(x)$. Цей метод має ту перевагу перед звичайною підстановкою, що він дає змогу відразу дістати коефіцієнти частки від ділення на x-r, якщо r буде коренем, і перейти до розгляду рівняння нижчого степеня.

Приклад. Розв'язати рівняння, знайшовши спочатку його раціональні розв'язки: $24x^4 - 37x^3 + 62x^2 - 74x + 28 = 0$.

Раціональними розв'язками тут можуть бути $\frac{p}{q}\left(\frac{28}{24}: \frac{\pm 1, \pm 2, \pm 4, \pm 7, \pm 14, \pm 28}{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24}\right)$:

$$\pm 1, \pm 2, \pm 4, \pm 7, \pm 14, \pm 28, \pm\frac{1}{2}, \pm\frac{7}{2}, \pm\frac{1}{3}, \pm\frac{4}{3}, \pm\frac{7}{3}, \pm\frac{14}{3}, \pm\frac{28}{3}, \pm\frac{1}{4}, \pm\frac{7}{4}, \pm\frac{1}{6}, \pm\frac{7}{6}, \pm\frac{1}{8}, \pm\frac{7}{8}, \pm\frac{1}{12}, \pm\frac{7}{12}, \pm\frac{1}{24}, \pm\frac{7}{24}.$$

	24	*-37*	*62*	*-74*	*28*
1	*24*	*-13*	*49*	*-25*	*3*

Згідно теореми 6 при *k=1* вираз $\frac{3}{p-q} \in Z$ (1).

Умові (1) задовольняють числа: $\pm 2,4,\pm\frac{1}{2},\frac{2}{3},\frac{4}{3},\frac{1}{4},\frac{7}{4},\frac{7}{6},\frac{7}{8}$.

	24	*-37*	*62*	*-74*	*28*
-1	*24*	*-61*	*123*	*-197*	*225*

При *k=-1* вираз $\frac{225}{p+q} \in Z$ (2). Умові (2) задовольняють числа: $\pm 2,4,\pm\frac{1}{2},\frac{2}{3},\frac{1}{4},\frac{7}{8}$.

	24	*-37*	*62*	*-74*	*28*
2	*24*	*11*	*84*	*98*	*216*

При *k=2* умову $\frac{216}{p-2q} \in Z$ задовольняють числа: $-2,4,\frac{1}{2},\frac{2}{3},\frac{7}{8}$.

	24	*-37*	*62*	*-74*	*28*
-2	*24*	*-85*	*232*	*-538*	*1104*

При *k=-2* умову $\frac{1104}{p+2q} \in Z$ задовольняють числа: $4,\frac{2}{3},\frac{7}{8}$. Перевіримо, які з цих чисел є розв'язками рівняння:

	24	*-37*	*62*	*-74*	*28*
$\frac{2}{3}$	*24*	*-21*	*48*	*-42*	*0*

Отже, $\frac{2}{3}$ є розв'язком рівняння і $24x^4-37x^3+62x^2-74x+28=$

$=\left(x-\frac{2}{3}\right)\left(24x^3-21x^2+48x-42\right)=3\left(x-\frac{2}{3}\right)(8x^3-7x^2+16x-14)$. Перевіримо чи буде $\frac{7}{8}$ коренем многочлена $P(x)=8x^3-7x^2+16x-14$.

	8	-7	16	-14
$\frac{7}{8}$	8	0	16	0

$\frac{7}{8}$ є коренем рівняння *P(x).*

Маємо $24x^4 - 37x^3 + 62x^2 - 74x + 28 = 3\left(x - \frac{2}{3}\right)\left(x - \frac{7}{8}\right)\left(x^2 + 2\right)$. Раціональними розв'язками рівняння будуть $x_1 = \frac{2}{3}$, $x_2 = \frac{7}{8}$. Ще два розв'язки отримаємо розв'язуючи рівняння $x^2 + 2 = 0$. $x_3 = i\sqrt{2}$, $x_4 = -i\sqrt{2}$.

Додаткові запитання:

1. Розв'язати рівняння, знайшовши спочатку його раціональні корені: $24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6 = 0$.
2. Як знаходити межі дійсних коренів алгебраїчних рівнянь?
3. Які наближені методи розв'язування алгебраїчних рівнянь ви знаєте?

Лекція 30. Будова простого розширення числового поля. Звільнення від ірраціональності в знаменнику дробу

Нехай дано довільну числову множину *M*. Очевидно, завжди знайдуться числові поля, які містять всі числа множини *M*, наприклад, поле комплексних чисел.

Мінімальним полем $P\{M\}$, що містить дану числову множину *M*, називається поле, яке є перетином усіх числових полів, що містять множину *M*.

Зрозуміло, що для будь-якої числової множини *M* мінімальне поле $P\{M\}$ завжди існує і є підполем довільного іншого поля, яке містить множину *M*.

Нехай Δ – деяке числове поле, і α – число, яке належить цьому полю $\alpha \bar{\in} \Delta$. Розглянемо мінімальне поле $P\{\Delta,\alpha\}$, яке містить Δ і α. Очевидно, $P\{\Delta,\alpha\}$ є розширенням поля Δ, причому мінімальним розширенням, яке містить α. Справді, всяке розширення поля Δ, яке містить α міститиме і $P\{\Delta,\alpha\}$ за означенням мінімального поля.

Відомо, що мінімальне розширення поля Δ, яка містить число $\alpha \bar{\in} \Delta$, називають розширенням поля Δ, утвореним приєднанням числа α, і позначають $\Delta(\alpha)$. Аналогічно можна розглядати розширення $\Delta(\alpha_1,...,\alpha_k)$, утворене приєднанням кількох чисел $\alpha_1,...,\alpha_k$ до поля Δ, тобто мінімальне поле $P\{\Delta,\alpha_1,...,\alpha_k\}$, яке містить як Δ, так і числа $\alpha_1,...,\alpha_k$. Розширення, утворені приєднанням одного числа, називаються *простими.*

<u>Означення 1.</u> Поле $\Delta(\alpha)$, утворене приєднанням до поля Δ числа α, алгебраїчного відносно поля Δ, називається простим алгебраїчним розширенням поля Δ.

Будова простого алгебраїчного розширення характеризується такою теоремою.

Теорема 1. Поле $\Delta(\alpha)$, утворене з поля Δ приєднанням кореня α,

незвідного у полі Δ многочленна n-го степеня

$$f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0,$$

складається з усіх чисел виду

$$\zeta = c_0 + c_1\alpha + ... + c_{n-1}\alpha^{n-1}, \qquad (1)$$

де $c_0, c_1, ..., c_{n-1}$ - довільні числа з поля Δ.

Наслідок. Якщо α - корінь многочленна другого степеня над полем Δ

$$f(x) = x^2 + px + q,$$

Причому $\alpha \bar{\in} \Delta$, то просте алгебраїчне розширення $\Delta(\alpha)$ поля Δ, утворене приєднанням числа α, складається з усіх чисел виду $a + b\alpha$, де a, b - довільні числа з поля Δ.

<u>Означення 2.</u> Якщо корінь α квадратного тричлена над полем Δ, то просте алгебраїчне розширення $\Delta(\alpha)$, утворене з поля Δ приєднанням до нього числа α, називається квадратичним розширенням поля Δ.

Знищення ірраціональності в знаменнику

Нехай дано дріб $\frac{p(\alpha)}{q(\alpha)}$, де $p(\alpha)$, $q(\alpha)$ – многочлени над полем Q, а α – ірраціональний корінь незвідного многочлена $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ з раціональними коефіцієнтами (при цьому $q(\alpha) \neq 0$). Слід виконати такі тотожні перетворення даного дробу, щоб позбутись ірраціональності у знаменнику.

Якщо $\deg q \geq n$, то, ділячи $q(x)$ на $f(x)$ з остачею, дістанемо рівність $q(x) = f(x) \cdot s(x) + r(x)$.

Підставляючи значення $x = \alpha$, дістанемо $q(\alpha) = r(\alpha)$, тому $\frac{p(\alpha)}{q(\alpha)} = \frac{p(\alpha)}{r(\alpha)}$, де $\deg r < \deg f$. Отже, завжди можна вважати степінь знаменника заданого дробу меншим за n. Але тоді зрозуміло, що $r(x)$ і $f(x)$ взаємно прості, адже $f(x)$ - незвідний многочлен.

Нехай тепер $\varphi_1(x)$ та $\varphi_2(x)$ – многочлени над полем Q, такі, що

$$\varphi_1(x) \cdot f(x) + \varphi_2(x) \cdot q(x) = 1. \qquad (2)$$

Тоді $\frac{1}{q(\alpha)} = \varphi_2(x)$ і

$$\frac{p(\alpha)}{q(\alpha)} = p(\alpha)\ \varphi_2(x). \qquad (3)$$

Таким чином, щоб знищити ірраціональність в знаменнику дробу $\frac{p(\alpha)}{q(\alpha)}$, де α - корінь незвідного многочлена $f(x)$, потрібно виконати наступні дії:

1. Замінити $q(x) = r(x)$, де $r(x)$ – остача від ділення $q(x)$ на $f(x)$;
2. Знайти многочлени $\varphi_1(x)$ та $\varphi_2(x)$, що задовольняють рівність (2);
3. Обчислити $\varphi_2(x)$ і подати дріб $\frac{p(\alpha)}{q(\alpha)}$ за (3).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Завало С.Т. Костарчук В.Н. , Хацет Б.І. Алгебра і теорія чисел. – К.: Вища школа, 1976. – 384с.
2. Завало С.Т., Левищенко С.С., Пилаєв В.В. Алгебра і теорія чисел: Практикум.-К.: Вища школа, 1986.-264с.
3. Костарчук В.М., Хацет Б.І. Курс вищої алгебри, вид. 3. - К.: Вища школа, 1969.
4. Курош А.Г. Курс высшей алгебры. — М.: Наука. — 1963.
5. Марач В.С., Крайчук О.В. Курс лекцій з алгебри. Основні поняття. Основні числові системи: Навч. посіб. – Рівне, РДГУ, 2003, -110 с.
6. Марач В.С., Крайчук О.В. Курс лекцій з лінійної алгебри.- Рівне, 2005.
7. Окунев Л.Я. Сборник задач по высшей алгебре. - М.: Просвещение.-1964.
8. Ляпин Е.С., Евсеев А.Е. Алгебра и теорія чисел. – М., Просвещение, 1978.
9. Уткіна С.В., Наришкіна Л.С. Алгебра і числові системи.-К., Вища школа, 1995.
10. Фадєєв Д.К., Сомінський І.С. Збірник задач з вищої алгебри. - К., Вища школа, 1971.
11. Фадеев Д.К. Лекции по алгебре. – М.: Наука, 1984.

ЗМІСТ

ВСТУП 3

Лекція 1. Бінарні відношення. Рефлексивні, симетричні, транзитивні бінарні відношення. Розбиття на класи. Фактор-множина 4

Лекція 2. Натуральні числа (аксіоми Пеано). Принцип математичної індукції 7

Лекція 3. Групи. Приклади груп. Основні властивості груп 9

Лекція 4. Підгрупи. Означення та критерій. Ізоморфізми та гомоморфізми груп. Основні властивості ізоморфізму 11

Лекція 5. Кільце. Підкільце. Приклади кілець 14

Лекція 6. Поле. Підполе. Приклади. Основні властивості полів. Поле дійсних чисел 19

Лекція 7. Поле комплексних чисел. Алгебраїчна та тригонометрична форма 23

Лекція 8. Системи лінійних рівнянь. Основні означення 28

Лекція 9. Арифметичний *n*-вимірний векторний простір. Лінійна залежність і лінійна незалежність множини векторів. Ранг і базис скінченної множини векторів 33

Лекція 10. Критерії сумісності системи лінійних рівнянь. Теорема про існування ненульового розв’язку лінійної однорідної системи рівнянь, яка містить *n* рівнянь і *n+1* невідому 37

Лекція 11. Означення та основні властивості визначників. Необхідні і достатні умови рівності визначника нулеві 39

Лекція 12. Знаходження оберненої матриці за допомогою елементарних перетворень та за допомогою алгебраїчних доповнень. Матричний спосіб розв’язування лінійних рівнянь 42

Лекція 13. Теорема Крамера 46

Лекція 14. Фундаментальна система розв’язків лінійної однорідної системи рівнянь. Теореми про існування фундаментальної системи розв’язків 48

Лекція 15. Означення та приклади векторного простору. Підпростори. Основні властивості векторного простору 50

Лекція 16. Базис та розмірність скінченновимірного векторного простору. Ізоморфізм векторних просторів..... 54

Лекція 17. Лінійні оператори. Власні значення і власні вектори лінійного оператора..... 57

Лекція 18. Теорема про зв'язок характеристичних коренів матриці *A* та власних значень лінійного оператора *A*. Зведення матриць до діагонального виду 61

Лекція 19. Теорема про ділення з остачею в кільці цілих чисел. Найбільший спільний дільник та найменше спільне кратне двох чисел і зв'язок між ними. Алгоритм Евкліда 63

Лекція 20. Прості числа. Нескінченність множини простих чисел. Основна теорема арифметики. Застосування канонічного розкладу чисел до знаходження *НСД(a,b), НСК[a,b]*..... 67

Лекція 21. Порівняння у кільці цілих чисел та їхні основні властивості. Повна та зведена система лишків. Т. Ейлера та Ферма..... 70

Лекція 22. Лінійні порівняння з однією змінною. Теорема про число розв'язків. Метод розв'язування лінійних порівнянь..... 75

Лекція 23. Застосування порівнянь до виведення ознак подільності.... 79

Лекція 24. Перетворення звичайного дробу в десятковий та визначення довжини періоду десяткового дробу 81

Лекція 25. Многочлени над полем. Теорема про ділення з остачею. *НСД* двох многочленів. Алгоритм Евкліда 85

Лекція 26. Факторіальність кільця. Факторіальність кільця многочленів над полем 93

Лекція 27. Алгебраїчна замкненість поля комплексних чисел. Канонічний розклад многочленна над полем комплексних чисел та його єдність..... 96

Лекція 28. Многочлени з дійсними коефіцієнтами. Спряженість

уявних коренів таких многочленів. Незвідні над полем дійсних чисел многочлени та канонічний розклад многочленів над полем дійсних чисел 99

Лекція 29. Многочлени над полем раціональних чисел. Цілі і раціональні корені многочленна з цілими коефіцієнтами. Незвідні над полем раціональних чисел многочлени 102

Лекція 30. Будова простого розширення числового поля. Звільнення від ірраціональності в знаменнику дробу 110

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 113