С. Торайғыров атындағы Павлодар мемлекеттік
университетінің ғылыми журналы
Научный журнал Павлодарского государственного
университета имени С. Торайгырова

1997 ж. құрылған
Основан в 1997 г.

ПМУ ХАБАРШЫСЫ

ВЕСТНИК ПГУ

ФИЗИКО-МАТЕМАТИЧЕСКАЯ СЕРИЯ

1 2013

Научный журнал Павлодарского государственного университета
имени С. Торайгырова

СВИДЕТЕЛЬСТВО
о постановке на учет средства массовой информации
№ 4533-Ж
выдано Министерством культуры, информации и общественного согласия
Республики Казахстан
31декабря 2003 года

МАЗМҰНЫ

СОДЕРЖАНИЕ

CONTENTS

ӘОЖ 51

Г. Ж. Әміренова, А. Н. Жұмаш**, М. Х. Хамитов***

ҰЛЫ МАТЕМАТИК Т. Ы. АМАНОВ

Мақалада қазақ халқының көрнекті математигі, физика-математика ғылымдарының докторы, Ғылым академиясының математика және механика институтының директоры Т. Ы. Амановтың өмірі және ғылыми жетістіктері қарастырылған.

Қазақ ССР ғылым академиясының корреспондент-мүшесі, физика-математика ғылымының докторы, профессор Төлеубай Ыдырысұлы Амановтың тоқсан жылдығына арналады (1923-1978).

Т. Ы. Амановтың ғылыми-педагогикалық қызметі Қазақстанда ғылымның жаңа бағыттарын, әсіресе математика саласын дамыту үшін қажетті алғышарттарды қалптастыру кезеңіне жатады.

Физика-математика ғылымдарының докторы, профессор, ҚазССР ҒА-ның корреспондент-мүшесі Төлеубай Ыдырысұлы Аманов өзінің ұйымдастырушылық қабілеті арқылы Республикадағы математика ғылымының жаңа бағыттарын дамытуға үлкен үлес қосқан тұлғалардың бірі. Функцияның классикалық теориясының өкілі математиканың осы саласында кандидаттық және докторлық диссертацияларын Стеклов атындағы ССРО ҒА-ның математикалық институтында академик С. М. Никольскийдің жетекшілігімен жазды. Қазақстанда функциялар теориясы бойынша бірінші ғылым докторы, Т. Ы. Аманов ҚазССР ҒА-ның математика және механика институтында математиканың фундаменталды бөлімі бойынша бірінші ғылыми бөлімшесін ұйымдастырып, функционалды талдау және функциялар теориясының зертханасын ашып, оны өмір бойы басқарып келді.

Математика және механика институтының докторы бола отырып, ол институтта ұсынылған ғылыми бағыттар тематикасын және жүргізуші ғылыми орталықтармен байланысын дамытуға және кеңейтуге бар күшімен әрекет етті. Ол тұстас ғалымдар еліміздің ғылым тарихында ерекше орын алады.

Т. Ы. Амановпен кездескен, оны танитын адамдардың жадында ол қарапайым, бір беткей адам ретінде сақталды. Өз табиғаты бойынша дарынды адам болған. Оның өмірбаянына үңілетін болсақ, осы жайттарға оп-оңай көз жеткізуге болады.

Т. Ы. Аманов Семей облысының Құрманқожа ауылында 1923 жылдың 25 тамызында, Ыдырыс пен Бақыт Амановтардың шаруалар отбасында дүниеге келген. Оның әкесі кейін теміржол жұмыскері болды, Ұлы Отан Соғысына (1941-1945) қатысты, зейнетке шығып, мосқал жасында, өзінің үлкен ұлы қайтыс болғаннан кейін жеті жылдан соң қайтыс болды. Амановтар отбасында Төлеубайдан басқа тағы оның әпкесі Нұрхия және кіші бауыры Әнуәрбек болды. Мектеп жасындағы куәлардың айтуы бойынша құрбылар арасында Төлеубай Аманов көпшілдігімен, шат жарқын мінезімен танымал болатын, поэзиямен, музыкамен шұғылданатын, өз күшімен ұйымдастырылған көркемөнерге белсенді қатысып, өзі өлеңдер жазып, өте көп оқыған.

Орта мектептің барлық сыныптарын мадақтау грамоталарымен аяқтаған.

Мектепті 1940 жылы Семей қаласында тәмәмдап, сол жылы ҚазМУ-нің физика-математика факультетіне түсіп, тек бірінші курсты ғана аяқтап үлгерді. 1941 жылы он сегіз жасар студент әскерге шақырылып, Чирчик қаласындағы қысқа мерзімді соғыс курстарына жіберіледі. Осы курстардан өткен соң, оны резервтегі жауынгер ретінде Семей қаласының әскери комиссариат қарамағына жіберді. Осында Т. Ы. Аманов 1941 жылдың қараша айынан бастап білім алуды Семей педагогикалық институтының физика-математика курсында жалғастырады. Бірақ та бір жылдан соң оның оқуы тағы үзіледі. 1943 жылдың қаңтар айында оны Алматы жаяу әскер училищесіне жібереді, одан кейін осы жылдың тамыз айында ол майданға аттанады. Майданда ол Екінші Украиналық майданның 110 атқыштар дивизиясының 310 гвардиялық атқыштар полкына түседі. Соғыста Т. Ы. Аманов танкке қарсы қару қолдану ротасының құрамында

қатысады. Т. Ы. Аманов сол кезде ең қызу майдандық бөлімдерінің біріне түседі. Днепр өзенінің маңында Кременчугтен төмен ауданда Украина ССР Кировоград облысының Онуфриев ауданының Куцеваловка ауылын алу кезіндегі шайқастарда 1943 жылдың 6 және 7 қазанында танкке қарсы қарудың отын есептеумен Т. Ы. Аманов пулемет нүктесін басып, қарсыластың танкке қарсы пушкасын істен шығарды. Дәл осы шайқаста қазанның сегізінші жұлдызында Т. Ы. Аманов артиллериялық снарядтың үшқынымен аяғын қатты жарақаттап алады. Осы шайқаста табысты әрекеттері үшін Т. Ы. Аманов және оның әскери жолдастарының бір қатары өкіметтік марапаттарға ұсынылған болатын. Бірақ тылдық госпитальға жіберілген Т. Ы. Аманов және оған тиісті жауынгерлік ордені соғыс жылдарында ұшыраса алмай қалады. Әскери госпитальда 4 ай жатып, әскер есебінен мүгедек ретінде шыққан Т. Ы. Аманов 1944 жылдың ақпан айында өз туған еліне оралады. Бірақ соғыс эпопеясы оның өмірінде мәңгі өшпес із қалдырды.

Соғыста күйген, бірақ рухы түспеген жиырма бір жасар Т. Ы. Аманов одан әрі өмірге деген орасан құштарлығымен өзінің бейбітшілік мамандығына оралады. Сол жылдың көктемінде педагогикалық институттың бағдарламасы бойынша мемлекеттік емтихандарын шұғыл түрде тапсырып, өзінің жоғары білімін аяқтайды. Жас майдангер маман сол кезде физика-математика факультетінің деканы болып тағайындалады. Осы лауазымда ол 1949 жылға дейін қызмет атқарады. Педагог мамандардың жетіспеушілігінен жас деканға математикалық емес курстарды меңгеріп жүргізуге, әртүрлі студенттік үйірмелерді (неміс тілі, философия) ұйымдастыруға тура келеді.

1950 жылы факультет жас мамандармен толғаннан кейін, Т. Ы. Аманов үш жылға институтты қалдырып, Мәскеудегі СССР ҒА В. А. Стеклов атындағы Математикалық институтының аспирантурасына түседі. Осы сәттен бастап оның функциялар теориясының Мәскеу мектебімен шығармашылық байланысы, оның белгілі өкілдерімен жолдастық қатынастары басталады және енді ешкашан үзілмейді. Аспирантура бойынша Т. Ы. Амановтың ғылыми жетекшісі профессор С. М. Никольский болған (бүкіл дүниежүзіне белгілі академиктің мектебі сол кезде өз ырғағын ала бастаған). Одан біраз уақыт бұрын қазіргі кезде оның атымен аталатын Н-класстар теориясы

құрастырылған болатын. Төлеубай Ыдырысұлына осы класстарға байланысты мәселелерді шешу ұсынылған болатын. Олардың бірі – Н-класстарды енгізудің негізгі теоремасының жақсарылмау мәселесі. Оған жақсартушылықты дәлелдеген кезде бұрын салынған қосымша шектеулерді шешуге және оның табиғи жағдайларында Н-класстарды енгізудің негізгі теоремасының жақсартылмауын көрсетуге жолы түседі. Диссертациялық жұмыста қарастырылған тағы бір мәселе бигармоникалық теңдеулер үшін бірінші шеттік есепті шешудің вариациялық әдісін негіздеуге және шекаралық шарттарға қатысты осы есептің шешу тұрақтылығын негізге енгізу теоремалары болатын. Ол ССРО ҒА Баяндамаларының 3 нөмірлерінде жарияланған болатын. Диссертация 1953 жылы ССРО МИАН Ғылыми кеңесінде қорғалды.

Төлеубай Ыдырысұлы С. М. Никольскийдің алғашқы шәкірттерінің бірі болды. Жиырма жеті жасар шалғай жерден келген аспирант жаңа ғана орталық университеттерін бітіріп келген көптеген жас мамандардан өзінің жүйріктілігімен ерекшеленетін. Төлеубай Аманов оған дейін белгісіз тақырыпқа кіріп, оның алдына қойған міндеттерді тез арада шешіп, өз мерзімінде кандидаттық диссертация жазған. Осы жолдардан Сергей Михайлович Никольскийдің өз оқушысы туралы құрметпен айтып, мүмкін болған кезде оған тән айқындық пен екпінімен оған деген өз қатынасын көрсеткеніне көз жеткіземіз.

Аспирантурадан кейін келесі 10 жыл ішінде Т. Ы. Аманов Семей педагогикалық институтында жоғары математика кафедрасының меңгерушісі лауазымында, оқу және ғылым жұмысы бойынша проректор, сонымен қатар институт директорының міндеттерін атқарып, білім беру жүйесінің ірі қайраткері болып жұмыс істеуін жалғастырады. Семей қалалық кеңестің горком партиясының депутаты және мүшесі болып тағайындалып, оларда білім беру мәселелерін қарастырады. Осыған орай ол мектепте және ЖОО-да оқыту әдістемелерінің мәселелерімен айналасады. Бұны оның көлемдік қолжазба материалдары дәлелдейді (өкінішке орай, сол кезде жүйеленбей және басылмай қалған). Осы кезеңде ол аспиранттық жұмыстар тақырыбын дамытуды жалғастырады. ССРО ҒА Хабаршысында, Семей педагогикалық институттың Ғылыми жазбаларында жарияланған, оның кандидаттық диссертациясында қарастырылған жұмыстардың мәселелері ары қарай зерттелуін табады.

Осы кезеңнің басында Төлеубай Ыдырысұлының өмірінде мәнді оқиғалар болады: 1954 жылы ол Нұрсипат Оразмұхамедқызы Смаиловаға үйленеді. Бұдан кейінгі жылдары жас отбасы Нұрлан, Нұргүл, Серік және Төлеугүл деген балалардың туғандарын тойлайды. Амановтың барлық балалары өз ата-анасының жолын қуып, математика саласында жұмыс істейді.

1963 жылдың ақпанында Т. Ы. Аманов жоғары математика кафедрасының аға ғылыми қызметкерінің лауазымына ауысады және үш жылға Мәскеуге Стеклов атындағы математика институтына аттанады. Он жыл ішінде енгізу теоремасы алға басты, функциялар теориясының өздік бөліміне – функционалды кеңістіктердің енгізу теориясына айналып, талдаудың әртүрлі мәселелерінде одан әрі кең пайдалануы қарастырылды.

Т. Ы. Аманов докторлық диссертациясымен айналысумен қатар, SB-кеңістіктер теориясын зерттеумен айналысты және функционалды кеңістіктер теориясының дәстүрлі мәселелеріне айналған барлық негізгі мәселелерді шешкен болатын. Докторлық диссертация 1967 жылы қорғалды. Диссертацияда алынған нәтижелері 1976 жылы жазылған «Басым болатын аралас туындымен дифференциалданатын функциялардың кеңістігі» деген монографиясында жүйелі түрде айтылған болатын.

1968 жылдың көктемінде Т. Ы. Аманов ҚазССР ҒА математика және механика институтына шақырылды. Институтта ол жаңа функционалдық талдау және функциялар теориясының зертханасын ұйымдастырып басқарды және сонымен қатар институт директорының орынбасары қызметіне тағайындалды. Осы жылдардан бастап республикада функциялар теориясы қарқынды дами бастады. Институтта функциялар теориясы бойынша семинарлар жұмыс істей бастады. Қазақ университетінде Т. Ы. Аманов функционалдық талдаудың жалпы курсын жүргізген және зертахана қызметкерлеріне функционалдық талдау және функциялар теориясы мен олардың қосымшалары бойынша жалпы және арнайы курстар оқыды. Сапарға бару жолымен Институт қабырғасында және Одақтың ірі ғылыми орталықтарында басым дәрежеде математиканың әртүрлі бағыттары бойынша мамандарды жеткілікті қарқынды дайындығы басталды.

1970 жылдан бастап Математика және механика институтының директоры қызметінде болып Т. Ы. Аманов Институтта ұсынылған математиканың салаларын кеңейтуге және ғылыми қызметкерлерді дайындау үрдісін нығайтуға маңызды ықпалын тигізді. Жұмыс бастылығына қарамастан, Төлеубай Ыдырысұлы SB-кеңістіктермен байланысты әртүрлі мәселелерін зерттеуді жалғастырды. Олардың кейбіреулері жоғарыда аталған 1976 жылы шыққан оның монографиясына енген болатын. Одан кейінгі еңбектері республикалық және одақтық баспаларда, конференциялар мен симпозиумдарда жарияланған болатын. Соңғы жұмыстарының бірінде ол өзінің ғылыми жастық шағының тақырыбына оралып, Лапластың жалпыланған операторы үшін шеттік есебін қарастырып, оны шешудің тұйық формуласын алады. Оның жеке басшылығымен осы жылдары оннан аса аспиранттар мен ізденушілер кандидаттық жұмыстарын қорғады. Оның ізбасарлар қатарына Фалалеев Л. П., Базарханов Б. Б., Маукеев Б. И., Калиев С. К., Уалиев С., Жусіпов К., Келтенова Р., Измаилов А. Л., Апышев О. Д., Хамитов М. Х. сияқты математиктер енеді. Т. Ы. Аманов 1953 жылдан 1972 жылға дейін математика саласында елуге жуық ғылыми еңбектер жазған.

Әсіресе Алматыда Т. Ы. Амановтың ынтасымен өткізілген, оларды ұйымдастыру және өткізудің барлық мәселелеріне оның белсенді қатысуымен өткен ірі математикалық форумдарды ерекше атап кету қажет. Енгізу теоремасы бойынша Бүкілодақтық сипозиум, Бірлескен Совет-Чехословак сипозиумы Қазақстанның жас математиктер мектебіне тек қана кең қатынастарды жасау мағынасында ғана емес, сонымен қатар ғылыми деңгейді жоғарлатуға және республикада өткізілетін зерттеулер тақырыбын кеңейтуге жағымды әсерді болды. Осы өкілді бүкілодақтық және халықаралық мағыналы симпозиумдерді Алматы қаласында өткізуді таңдауға басым дәрежеде Т. Ы. Амановтың рөлі болды. Қазақстан Республикасының Ғылым академиясының вице-президенті, оның ісін Математика және механика институтының директоры ретінде жалғастырған академик Сұлтанғазин У. М. атақты математиктер С. Л. Соболевтің, С. М. Никольскийдің, А. Куфнердің, Нечастың (Чехословакия) және тағы басқалардың жарқын баяндамаларымен шыққандарын әлі де есінде сақтап қалған. Сұлтанғазин У. М. сөздерінен: «Төлеубай Ыдырысұлы Ванкуверде

(Канада) халықаралық математикалық конгресіне қатысты. Осындай катынастар тығыз байланыстарды енгізуге және ғылыми зерттеулер деңгейлерін жоғарлатуға себеп болды. Төлеубай Аманов атақты ғалым, ғылым ұйымдастырушысы, педагог және керемет адам болды. Оған қарапайымдылық және ақиқаттылық сияқты адам қасиеттері тән болды. Оның өмір жолы – ғылым мен отан үшін қызмет ету жолы – жас ұрпақ үшін үлгі. Төлеубай Амановқа құрмет міндетін бере отырып, Қазақ Ғылым академиясы таза танымдық математикалық мәселелеріне арналған зерттеулер тоқталмайды және өз приоритеттерін сақтап қалады деп үміттенемін».

Оны білетін ресейлік математиктер арасында Төлеубай Ыдырысұлы үнемі үлкен құрметке ие болатын. Осыған орай С. Л. Соболевтің Қазақ ССР ғылым академиясына Ғылымдар академиясының корреспондент-мүшелеріне Т. Ы. Амановтың кандидатурасын қолдау үшін жазған хатын ұсына кетейік: «Ғылымдар академиясының корреспондент-мүшелеріне Т. Ы. Амановтың кандидатурасын қолдаймын. Амановтың енгізу теоремасы бойынша, дербес туындылардағы теңдеулер теориясы және аралас туынды мәселелері бойынша зерттеулерін жақсы білемін. Оның арқасында қазақ Ғылым Академиясы белсенді жұмыс істейтін математикті, қызық және терең өзіндік шығармашылық жетістіктерге ие болатын, математикалық талдаудың үлкен және маңызды саласының керемет білгішіне ие болады. Академик Соболев. 15 мамыр 1969 жыл».

Белгілі ғалым, педагог, ұйымдастырушы Т. Ы. Амановтың көпқырлы қызметі оның нағыз шарықтап тұрған шағында үзіліп қалды. Оның өмірден озуы Қазақстандағы математика ғылымы үшін бірден сезілді. Бірақ, оның өз өмірін арнаған ісі бүгін де жалғасын тауып отыр. Қазір Республиканың барлық ірі орталықтарында функциялар теориясы және функционалдық талдау саласында табысты жұмыс жасалып, жақсы мамандар, тіпті мектептер де бар. Оның туған ауылында өзі оқыған мектеп пен Семей қаласындағы көше Т. Ы. Амановтың атымен аталды. Т. Ы. Амановтың жетпіс жылдығына орай соңғы жылдары тұрған үйдің қасында мемориалды тақта орнатылды. Амановқа арналған ғылыми конференцияларды өткізу дәстүрге айналып отыр. 1983 және 1993 жылдары республиканың ғылым академиясының математика институты Төлеубай Ыдырысұлының алпыс және жетпіс жылдығын

ғылыми конференцияларды өткізуімен атап өтті. 1998 жылы Е. А. Букетов атындағы Қарағанды Мемлекеттік Университеті Т. Ы. Амановтың жетпіс бес жылдығына арналған функционалдық кеңістіктерді енгізу және жуықтату теориясы бойынша республикалық конференциясын өткізді. 2003 жылы Амановтың 80 жылдығына арналған конференция Семейде өткізілді. Бүгінгі таңда жас ұрпақ оның ісін жалғастырып, оның есімін мәңгі есінде сақтайды.

Осы жылы біз Төлеубай Ыдырысұлы Амановтың тоқсан жылдық мерейтойын тойлаймыз. Біз Т. Ы. Амановты тек қана көрнекті математик және математиканы жан-жақты жақсы меңгерген ғалым ретінде ғана емес, сонымен қатар кең пейілді, адамгершілігі мол адам ретінде танимыз.

Т. Ы. Амановты оның жолдастары, әріптестері, оқушылары мәңгі жадында сақтап, оның ғылымға деген бағаланбас үлесі туралы жас ұрпаққа жеткізіп, өз кезегінде Төлеубай Ыдырысұлы Амановпен қызметтес болғанын, оның математика саласына үлкен үлес қосқанын мақтанышпен айтады.

ӘДЕБИЕТТЕР ТІЗІМІ

1 **Аманов, Т. Ы.** Пространства дифференцируемых функции с доминирующей смешанной производной. – Алматы, 1976 г.

2 Международная научно-практическая конференция. Теория функций, функциональный анализ и их приложения. – Семей, 2003 г.

*Абай атындағы мектебі, Лебяжі ауданы, Павлодар облысы;
**С. Торайғыров атындағы Павлодар
мемлекеттік университеті, Павлодар қ.
Материал 09.05.13 редакцияға түсті.

Г. Ж. Амренова, А. Н. Жумаш**, М. Х. Хамитов***

Великий математик Т. Ы. Аманов

*Средняя школа имени Абая, Лебяжинский р-н, Павлодарская обл.;
**Павлодарский государственный университет
имени С. Торайгырова, г. Павлодар.
Материал поступил в редакцию 09.05.13.

G. Zh. Amrenova, A. N. Zhumash**, M. Kh. Khamitov***

Eminent mathematician T. Y. Amanov

*Secondary school after Abai, Lebjazhje district, Pavlodar region;
**Pavlodar State University named after S. Toraigyrov, Pavlodar.

Material received on 09.07.13.

Данная статья повествует о жизни и научных достижениях известного казахстанского математика, доктора физико-математических наук, директора Института математики и механики Академии наук.

This article is about life and scientific achievements of well-known mathematician of Kazakh people, doctor of physics-mathematics science, director of mathematics and mechanics institute of science academy.

УДК 372.851

Ф. С. Алдабергенов

О МЕЖПРЕДМЕТНОЙ СВЯЗИ МЕЖДУ ГЕОМЕТРИЕЙ И ЧЕРЧЕНИЕМ

В статье излагается межпредметная связь между геометрией и черчением.

Межпредметная связь в процессе обучения в школе – необходимое условие успешного преподавания. От того, как осуществляется эта связь в школе, зависит развитие мышления учащихся, их кругозор; насколько сознательно будут применяться полученные ими знания в жизненных ситуациях. У школьника формируется целостная картина мира, общее представление о законах природы и о развитии общества в условиях рыночной экономики. В процессе обучения в школе каждым учеником будет прочувствована связь между математикой и другими дисциплинами, как в содержании, методах, так и в приемах обучения. Нельзя забывать, что математика – основа современной мысли.

Ее богатства используются в самых различных областях научного знания. Без математики трудно порой обойтись при изучении дисциплин, казалось бы, далеких от математики.

Черчение и геометрия. Эти две школьные дисциплины занимаются изучением пространственных форм и пространственных отношений материального мира. Связь между геометрией и черчением обусловлена тем, что геометрия дает теоретические основы для черчения, а навыки построения, полученные в процессе обучения черчению, используются на уроках геометрии. Учитель черчения должен опираться на теоретические сведения, известные учащимся из курса геометрии, равно как и учителю геометрии следует больше обращать внимание на вопросы, связанные с построениями.

На необходимость использования разнообразных приемов работы чертежными инструментами для решения геометрических задач указывал в свое время геометр Н. Ф. Четверухин. Ранее об этом говорилось в труде аль-Фараби «Приемы циркуля и линейки». Эта книга давала необходимые научные основы для овладения азбукой инженерного дела – черчения. В трудах советских ученых Н. А. Рынина, А. И. Добрякова, В. О. Гордона, Н. Ф. Четверухина методы начертательной геометрии получили большое развитие и применение во многих областях науки, техники и искусства.

О применении построения геометрических фигур и тел, сечения геометрических тел плоскостью для нахождения натуральных величин отрезков при решении математических задач будет излагаться в данной работе как метод наглядной самопроверки через графику.

Пожелания многих учителей – установление межпредметных связей, когда в программах разных учебных предметов соответствующие разделы будут изучаться одновременно, т. е. когда будет соблюдаться так называемая синхронность. Однако практика показала, что в силу объективных причин в школьных программах не удается достичь такого положения. Поэтому необходимо определить тот минимум геометрических понятий и утверждений (теоремы синусов и косинусов, подобие треугольников, теорема Пифагора, площади геометрических фигур и объемы геометрических тел), которыми учащиеся должны овладеть для сознательного усвоения предмета черчения в 9 классе. Школьники старших классов часто не различают

такие понятия как «ребро», «грань», «вершина», отличительные особенности в условностях и обозначениях. Наглядность, «зримость» этих элементов как на предмете, так и на его чертеже является необходимостью, облегчающей усвоение понятий, связанных с ними.

Систематическое ознакомление учащихся с геометрическими свойствами пространственных фигур и взаимосвязью между их элементами приводит к обобщению первоначальных пространственных представлений и формированию геометрических понятий. Процесс накопления и расширения запаса пространственных представлений протекает наиболее успешно в условиях интеграции двух предметов (геометрии и черчения). В этом отношении существенная роль может принадлежать графическим способам решения геометрических задач. При решении комплексной графической задачи (на вычисление или построение) учащиеся должны, во-первых, мысленно представлять пространственную фигуру, описанную в условии задачи, во-вторых, начертить ее наглядное изображение (аксонометрию).

Выполнение этих требований нередко оказывается весьма трудным для учащихся. Однако условие задачи сопровождается обычным наглядным рисунком фигуры, которую можно изобразить ортогональной проекцией чертежа фигуры на трех плоскостях проекции $П_1$, $П_2$ и $П_3$, где $П_1$ – горизонтальная плоскость проекции, $П_2$ – фронтальная плоскость проекции, $П_3$ – профильная плоскость проекции.

В стереометрии нередко приходится рассматривать сечения тел, в частности многогранников, различными плоскостями. Обычно задача состоит в том, чтобы построить сечение, имея параллельную проекцию тела. Приведем некоторые соображения, которыми пользуются при построении сечений многогранников. Прежде всего заметим, что сечение выпуклого многогранника есть выпуклый плоский многоугольник, вершины которого в общем случае являются точками пересечения секущей плоскости с ребрами многогранника, а стороны многоугольника получаются при пересечении секущей плоскости с гранями многогранника. Для построения прямой, по которой пересекаются плоскости, обычно находят две ее точки и проводят через них прямую. Для построения точки пересечения прямой и плоскости находят в плоскости прямую, пересекающую

данную. Тогда искомая точка получается в пересечении найденной прямой с данной. Приведем пример, из которого видно, как применяются эти соображения.

Задача из учебника геометрии А. В. Погорелова (1988 г.) для 6-10 классов. В правильной шестиугольной призме, у которой боковые грани – квадраты, проведите плоскость через сторону нижнего основания и противолежащую ей сторону верхнего основания. Сторона основания равна a. Найдите площадь построенного сечения.

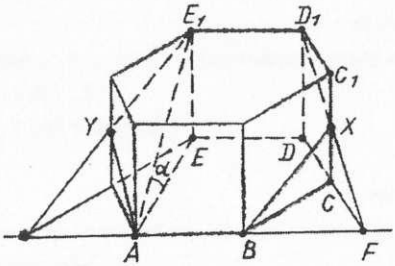


Рисунок 1 – Наглядное изображение пространственной фигуры

Решение. Сечение проходит через параллельные прямые AB и E¹D¹ (рис.1). Ребра AB и E¹D¹ являются сторонами многоугольника в сечении. Найдем сторону D¹X этого многоугольника, лежащую в грани CC¹D¹D. На прямой D¹X мы знаем одну точку D¹. Другой точкой является F - точка пересечения прямых AB и CD. Она лежит в плоскости грани CC¹D¹D и в плоскости сечения, а значит и на прямой их пересечения D¹X. Соединяя точки D¹ и F прямой, получим точку X. Отрезок D¹X есть сторона сечения в грани CC¹D¹D. Аналогично находим точку Y. Искомый многоугольник в сечении есть ABXD¹E¹Y.

Найдем теперь площадь сечения. Шестиугольник в основании призмы является ортогональной проекцией шестиугольника в сечении. Поэтому площадь сечения $S = \frac{S_0}{cos\alpha}$ где S_0 - площадь основания призмы, а α - угол, который образует секущая плоскость с плоскостью основания. Так как $EA \perp AB$, то $E^1A \perp AB$ (теорема о трех перпендикулярах). Поэтому α равен углу EAE¹. А так как $EE^1 = a$ и

$AE = a\sqrt{3}$, как сторона правильного треугольника AEC, вписанного в окружность радиуса a, то $AE^1 = \sqrt{a^2 + (a\sqrt{3})^2} = 2a$. Поэтому $cos\alpha = \frac{a\sqrt{3}}{2a} = \frac{\sqrt{3}}{2}$. Площадь основания призмы равна $S_0 = 6 \cdot \frac{1}{2}a^2 sin60° = 3a^2\frac{\sqrt{3}}{2}$. Тогда площадь сечения $S = \frac{S_0}{cos\alpha} = 3a^2$.

Средняя школа № 12, г. Экибастуз.
Материал поступил в редакцию 26.08.13.

Ф. С. Алдабергенов

Геометрия мен сызу арасындағы пәнаралық байланыс туралы

№ 12 орта мектебі, Екібастуз қ.
Материал 26.08.13 редакцияға түсті.

F. S. Aldabergenov

About interdisciplinary connections between geometry and drawing

№ 12 secondary school, Ekibastuz.
Material received on 26.08.13.

Бұл мақалада геометрия мен сызу арасындағы пәнаралық байланыс жазылған.

The article describes the interdisciplinary connections between geometry and technical drawing.

УДК 373.51

А. И. Баланюк

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ИНДИВИДУАЛИЗИРОВАННОГО СПОСОБА ОБУЧЕНИЯ НА УРОКАХ МАТЕМАТИКИ

Обучение на основе новых педагогических технологий, базирующихся на деятельностном подходе, чтобы ученик непрерывно овладевал жизненно важными способами деятельности, ключевыми компетенциями, мог проявить активность, самостоятельность – задача сегодняшнего образования. Технология индивидуализированного способа обучения дает возможность реализации данной задачи. В статье представлена система деятельности и опыт учителя при работе по ТИСО на уроках математики.

Урок – главная составная часть образовательного процесса. Учебная деятельность учителя и учащихся в значительной мере сосредотачивается на уроке. Вот почему качество подготовки учащихся по той или иной учебной дисциплине во многом определяется уровнем проведения учебного занятия.

Непременным условием успешности учителя является владение современными образовательными технологиями и внедрение их в свою практику.

При подготовке и проведении учебного занятия отправными точками для каждого педагога современной школы должны стать следующие принципы: урок – это открытие, поиск и осмысление истины. Стратегия современного урока далеко выходит за пределы простой передачи знаний. Знание является только его содержанием, ключевой результат – развитие интеллекта и духовное обогащение каждого участника образовательного процесса; урок – это часть жизни ребенка, и проживание этой части должно совершаться на уровне высокой общечеловеческой культуры. Если на уроке изучается истина, высвечивающая одну из сторон жизни, значит, изучается сама жизнь. При таком подходе меняется отношение школьника к

обучению, иным образом конструируется процесс обучения; высшей ценностью на уроке является человек [1].

В педагогике неизбежно возникают вопросы: "чему учить?", "зачем учить?", "как учить?", но, вместе с тем, появляется еще один: "Как учить результативно?"

По мнению Г. К. Селевко, "любая технология имеет средства, активизирующие и интенсифицирующие деятельность учащихся, в некоторых же технологиях эти средства составляют главную идею и причину эффективности результатов" [2].

Поэтому целью моей работы в плане «обновления содержания образования» является создание оптимальных условий для самостоятельной деятельности учеников, которая направлена на индивидуальную самореализацию и развитие личностных качеств с одновременным высоким уровнем освоения ими содержания преподаваемого предмета математики.

Исходя из основной цели, поставлена следующая задача: построить обучение школьников на основе новых педагогических технологий, базирующихся на деятельностном подходе, чтобы ученик непрерывно овладевал жизненно важными способами деятельности, ключевыми компетенциями, мог проявить активность, самостоятельность. Одной из таких технологий, применяемой в практике, является технология индивидуализированного способа обучения (ТИСО), при освоении которой основное внимание уделяется созданию условий для работы с каждым в отдельности учеником с учетом индивидуальных познавательных возможностей, потребностей, интересов. Данная технология успешно внедряется в практику работы преподавателей разных учебных дисциплин, в том числе и математики.

Какова же система действий учителя при работе по ТИСО?

На основе стандарта содержания темы выстраивается система целей обучения по данной теме. Главным является четкое представление о требованиях стандарта к подготовке учащихся, что дает возможность для целенаправленной организации процесса обучения и системного контроля оценки знаний учащихся. После этого формируется комплексная дидактическая цель, которая имеет два уровня: уровень усвоения учебного содержания учеником и

ориентация на его использование в практике, а также для изучения учебного материала в будущем [5].

Например, предлагается урок математики в 5 классе по ТИСО.

УЧЕБНЫЙ ЛИСТ по теме: «Уравнения» (3 занятия)

ЗАДАНИЕ №1

Прочитай и выучи **определение:** Уравнением называют равенство, содержащее букву, значение которой надо найти.

Решить уравнение – значит найти все его корни или убедиться, что это уравнение не имеет корней.

Значение буквы, при котором уравнение становится верным числовым равенством, называется корнем уравнения.

Например: $5x + 8 = 28$ – уравнение. $x = 4$ 4 – корень уравнения. **(2б)**

1. Реши четные или нечетные уравнения **(6 б):**

1. $x + 13 = 52$; 5) $51 - y = 36$ 9) $15y = 75$
2. $x + 16 = 55$; 6) $78 - y = 42$ 10) $25y = 125$

ПРОЙДИ ПРОВЕРКУ №1.

ЗАДАНИЕ №2

1. Рассмотри примеры решения уравнений: **(3 б)**

1.$(x-3)9=72$ В заданном уравнении неизвестен множитель $x+3$.

$x-3=72:9$ Чтобы найти неизвестный **множитель**, нужно произведение $x-3 = 8$ разделить на известный множитель.

$x=8+3$ Решаем уравнение $x-3 =8$. Здесь неизвестно уменьшаемое.

$x=11$. Чтобы найти неизвестное уменьшаемое, нужно сложить разность и вычитаемое. Ответ: 11 – корень уравнения.

2. Выполни по образцу 1 или 2 столбик: **(6б)**

1) $(x-6)12 = 72$ 4) $(x-5)13 = 65$
2) $(12-x)8 = 32$ 5) $(19-x)7 = 49$
3) $85(x+3) = 17$ 6) $68(x+2) = 17$

ПРОЙДИ ПРОВЕРКУ №2.

ЗАДАНИЕ № 3

Рассмотри алгоритм решения задачи с помощью уравнения: **(2б)**

1. Выбрать неизвестную величину, которую обозначим буквой x (или какой-нибудь другой строчной буквой латинского алфавита);

2. Составить уравнение по содержанию задачи;

3. Решить уравнение.

4. Ответить на вопрос задачи, проверить правильность решения задачи.

1) Реши задачу на выбор. **(3б)**

1. С пришкольного участка ученики за два дня собрали 360 кг моркови. Во второй день ученики собрали в 2 раза больше моркови, чем в первый день. Сколько килограммов моркови собрали ученики в первый день?

2. За два дня в магазине продали 480 кг овощей. В первый день продали на 60 кг больше, чем во второй день. Сколько килограмм овощей продали во второй день?

ПРОЙДИ ПРОВЕРКУ № 3

Молодец! Теперь ты можешь приступать к **проверочной работе №1.**

ЗАДАНИЕ №4

1. Найди корни уравнения, решив 1, 2 или 3 вариант. **(6б)**

1 вариант	2 вариант	3 вариант
1. $(12m-5m)4 = 252;$	1) $(4n+3n)11 = 154;$	1) $(17n-8n)13 = 351;$
2. $45:(4m-m) = 3;$	2) $(19n-6n):4 = 26;$	2) $(16m+5m):18 = 7;$

2. Реши одну из задач с помощью уравнения: **(4б)**

а) Мадина и Зинура при оформлении багажа в аэропорту узнали, что вес сумок Мадины в 2 раза меньше веса сумок Зинуры. Мадина добавила в свои сумки 3 кг, после чего общий вес сумок стал 36 кг. Сколько килограммов весили сумки Мадины первоначально?

б) Марат и Асхат помогали бабушке собирать на даче яблоки. Марат собрал в 4 раза яблок больше, чем Асхат. В корзину Асхата ребята доложили еще 15 яблок, после чего в двух корзинах стало всего 70 яблок. Сколько яблок собрал Асхат первоначально?

ПРОЙДИ ПРОВЕРКУ № 4.

ЗАДАНИЕ № 5

1) Составь задачу по уравнению (на выбор) и реши его. **(4б)**

1) $250 - 3y = 115;$ 2) $(48 - x) : 8 = 4.$

2) Угадай корень уравнения $10 - x \cdot x = 1$ и выполни проверку. **(4б)**

ПРОЙДИ ПРОВЕРКУ № 5

Молодец! Теперь ты можешь приступать к **проверочной работе №2.**

Таблица 1 – РЕЙТИНГОВЫЙ ЛИСТ по теме: «Уравнение»

Ф.И.О. _____, класс _____

№	max баллов	Полученный балл	Кто проверил	Кого проверил	Оценка
1	2				
	6				
2	3				
	6				
3	2				
	2				
	3				
Проверочная работа №1	18				
4	6				
	4				
5	4				
	4				
Проверочная работа №2	10				
Итого	70				

Итого: 70 баллов,«5» – 65-70 б.,«4» – 58-64 б.,«3» – 52-57 б.

Он является самоучителем по теме. Задания разрабатываются в соответствии с содержанием учебника. В них предусмотрены все уровни усвоения учебного материала: репродуктивный, реконструктивный и творческий. Причем, учебный лист составляется единый для всех учеников. В системе заданий предполагается промежуточный и итоговый контроль результатов обучения.

При этом учащийся учится сам, а учитель осуществляет мотивационное управление его учением: мотивирует, координирует, консультирует и контролирует. В технологии применяется самооценка, которая приучает ребенка объективно оценивать свои способности, результаты своего труда. Учащийся максимальное время работает самостоятельно, учится целенаправленно. Это дает возможность

осознать себя в деятельности, учит самоорганизации, самооценке, позволяет каждому учащемуся видеть уровень усвоения знаний.

Как организуется деятельность в ТИСО?

Важным критерием построения занятия являтся вводный (организационный) модуль, который определяет четкое взаимодействие учителя и учеников, когда проводится инструктаж учителя. Далее самостоятельная работа учеников, проверка выполненного учителем, взаимообучение, взаимопроверка, индивидуальная коррекция результатов, промежуточный контроль, планирование домашней работы, ведение рейтингового листа темы.

Учитель, подводя итоги деятельности ученика на основе рейтингового листа темы, имеет возможность логического перехода от дифференциации к индивидуализации работы с учащимся.

Проверка всех видов работ производится на самом уроке самим учеником посредством самопроверки, взаимопроверки, проверки некоторых видов работ учителем. Каждый вид работы имеет свою оценку, которую ученик выставляет непосредственно в лист рейтинговой оценки. Конечно, ученик есть ученик. Он может пойти на уловки при самопроверке. Но при перепроверке учителю будет видна объективность проверки. Кроме того, общая оценка за урок будет подтверждена контрольной итоговой работой, которую учитель проверяет сам.

Преимущества данной формы работы в том, что ученик непосредственно сам выявляет свои ошибки, пробелы знаний тут же по результатам проверяемого материала, знает, какие "дыры следует латать". Он сам контролёр своих знаний.

Подсчёт оценочных баллов в окружении подсчёта другими одноклассниками своих работ психологически создаёт ситуацию азарта, возможности накопления балла, создающего ситуацию успеха.

Учитель детально видит каждого ученика на каждом уроке. Такая оценка работы каждого учащегося решает также и проблему накопляемости оценок по предмету.

Опыт работы с технологией показывает, что данный вид обучения позволяет успешно решать следующие задачи: повышает сознательность и прочность усвоения знаний учащихся; вырабатывает у школьников умение самостоятельно приобретать новые знания из разных источников,

глубоко осмысливать их и включать в систему; прививает школьникам культуру умственного труда и учит их самостоятельно трудиться продуктивно, с интересом подходить к достижению поставленной цели; готовит учащихся к тому, чтобы они могли эффективно заниматься самообразовательной работой в дальнейшем.

Основной оценкой эффективности технологии является успеваемость учащихся. Работа по технологии ТИСО позволяет достичь высокого уровня мотивации учащихся, реализации самостоятельности и возможности для учащихся усвоить учебный материал в своем темпе и на своем уровне. В ходе работы создается атмосфера соревнования, темпа, стимула, ситуации успеха. Кроме осознания своего успеха, ТИСО позволяет осуществить принцип здоровьесбережения. Здоровье ребенка зависит от успешности его деятельности. Так как задания по данной технологии выбираются в соответствии со способностями, без ограничения во времени для решения задач, что создает психологический комфорт в обучении.

И самое главное с самого начала иметь «инструмент взятия знаний», которым смогли бы организовать свое восприятие, внимание к знаниям, их понимание, поиск и воспроизведение, то есть постепенное формирование своих личных способов обучения, методов познания. Данная технология позволяет учителю и ученику развиваться вместе, учитель стоит не над учеником, а вместе с ним.

СПИСОК ЛИТЕРАТУРЫ

1**Иванова, Т. Н.** Технология индивидуализированного способа обучения (ТИСО) как средство реализации личностно – ориентированного обучения. «Валихановские чтения 9». – Кокшетау, 2004. – с. 83-86.

2**Селевко, Г. К.** Современные образовательные технологии: Учебное пособие. – М. : Народное образование, 1998.

3Учебная программа «Математика» для 5-6 классов общеобразовательной школы – Астана, 2010.

4Учебник: Математика 5 класс. Т. А. Алдамуратова. – Алматы: «Атамұра», 2005.

5Научно-практический журнал // «Школьная технология», №4. – 2009.

Средняя общеобразовательная школа № 43, г. Павлодар.
Материал поступил в редакцию 29.04.13.

А. И. Баланюк

Математика сабақтарында оқытудың дербестендірілген тәсілі технологиясын қолдану

№ 43 ЖОМ, Павлодар қ.
Материал 29.04.13 редакцияға түсті.

A. I. Balanyuk

Using the technology of individualized learning way in math lessons

№ 43 secondary comprehensive school, Pavlodar.
Material received on 29.04.13.

Бүгінгі таңда білім берудің мақсаты – жаңа педагогикалық технологиялардың негізінде оқушы үздіксіз тіршілікке маңызды әдістерімен, басты құзырларымен дербестік, белсенділік көрсету арқылы меңгеру. Оқытудың дербестендірілген тәсіл технологиясы бұл тапсырманы жүзеге асыруға мүмкіндік береді. Мақалада математика сабақтарында оқытудың және жүйесі техникасы бойынша жұмыста қызмет жүйесі және мұғалімнің тәжірибесі көрсетілген.

Training on the basis of the new pedagogical technologies based on the activity approach so that a student continuously masters the vital ways of activity, key competence, could show activity, independence which are of today's education. The technology of the individualized method of training gives the chance to realization of the given problem. Working system and experience of the teacher working on the technology of individualized way of learning in math lesson.

ӘОЖ 378.51

В. О. Будкова, И. И. Павлюк, А. Ф. Зейнулина

ТЕТРАЭДРЛАР ТОБЫНЫҢ ТҮЙІНДЕС ЭЛЕМЕНТЕР КЛАСЫНЫҢ ГРАФЫ

Бұл жұмыста тетраэдрлар тобы түсінігі түйіндес элементтер класының графтары арқылы берілген. Негізі түсініктер мен анықтамаларды [1,2,3,4] жұмыстардан танысуға болады.

$T=\{e,a,a^2,b,ab,ba,a^2b,ba^2,aba,bab,a^2ba,aba^2\}$ тетраэдрлар тобында он екі элемент және $(ab)^3=e$, $a^3=e$, $(ab)^2=ba^2$, $b^2=e$ генетикалық код бар. Осы топты топтардың түйіндес элементтер кластарын пайдаланып граф арқылы түсіндіреміз.

$$e=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} \quad a_4=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix} \quad a_8=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$$

$$a_1=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix} \quad a_5=\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix} \quad a_9=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

$$a_2=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} \quad a_6=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix} \quad a_{10}=\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$$

$$a_3=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} \quad a_7=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} \quad a_{11}=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$$

1 кесте

	e	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}
e	e	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}
a_1	a_1	a_2	e	a_{11}	a_5	a_8	a_{10}	a_6	a_9	a_5	a_7	a_4
a_2	a_2	e	a_1	a_4	a_{11}	a_9	a_7	a_{10}	a_5	a_8	a_6	a_3
a_3	a_3	a_5	a_{10}	e	a_8	a_1	a_{11}	a_9	a_4	a_7	a_2	a_6
a_4	a_4	a_9	a_6	a_2	a_5	e	a_3	a_8	a_{11}	a_{10}	a_1	a_7
a_5	a_5	a_{10}	a_3	a_6	e	a_4	a_2	a_{11}	a_7	a_1	a_9	a_8
a_6	a_6	a_4	a_9	a_5	a_7	a_{10}	a_8	a_1	e	a_{11}	a_3	a_2
a_7	a_7	a_{11}	a_8	a_9	a_{10}	a_6	a_5	e	a_2	a_3	a_4	a_1
a_8	a_8	a_7	a_{11}	a_{10}	a_1	a_3	e	a_4	a_6	a_2	a_5	a_9

a_9	a_9	a_6	a_4	a_7	a_2	a_{11}	a_1	a_3	a_{10}	e	a_8	a_5
a_{10}	a_{10}	a_3	a_5	a_8	a_6	a_7	a_9	a_2	a_1	a_4	a_{11}	e
a_{11}	a_{11}	a_8	a_7	a_1	a_9	a_2	a_4	a_5	a_3	a_6	e	a_{10}

$T=\{e, a, a^2, b, ab, ba, a^2b, ba^2, aba, bab, a^2ba, aba^2\}$

Топтың генетикалық коды: $a^3=b^2=(ab)^3=e$; $(ab)^2= ba^2$

2 кесте – T_{12}-ші топ элементтерінің Кэли кестесі

	e	a	ab	ba	bab	b	a^2ba	aba^2	a^2	aba	ba^2	a^2b
e	e	a	ab	ba	bab	b	a^2ba	aba^2	a^2	aba	ba^2	a^2b
a	a	a^2	a^2b	aba	ba^2	ab	ba	bab	e	a^2ba	aba^2	b
ab	ab	aba	ba^2	a^2	a^2b	a	bab	ba	aba^2	b	e	a^2ba
ba	ba	ba^2	aba	a^2b	a^2	bab	a	ab	b	aba^2	a^2ba	e
bab	bab	a^2b	a^2	ba^2	aba	ba	ab	a	a^2ba	e	b	aba^2
b	b	ba	bab	a	ab	e	aba^2	a^2ba	ba^2	a^2b	a^2	aba
a^2ba	a^2ba	bab	ba	ab	a	aba^2	e	b	a^2b	ba^2	aba	a^2
aba^2	aba^2	ab	a	bab	ba	a^2ba	b	e	aba	a^2	a^2b	ba^2
a^2	a^2	e	b	a^2ba	aba^2	a^2b	aba	ba^2	a	ba	bab	ab
aba	aba	aba^2	a^2ba	b	e	ba^2	a^2	a^2b	ab	bab	ba	a
ba^2	ba^2	b	e	aba^2	a^2ba	aba	a^2b	a^2	ba	a	ab	bab
a^2b	a^2b	a^2ba	aba^2	e	b	a^2	ba^2	aba	bab	ab	a	ba

$|e|=1$ $\quad$ $|a^2ba|=2$

$|a^2|=3$ $\quad$ $|aba^2|=2$

$|ba^2|=3$ $\quad$ $|a|=3$

$|a^2b|=3$ $\quad$ $|bab|=3$

$|aba|=3$ $\quad$ $|ab|=3$

$|b|=2$ $\quad$ $|ba|=3$

Ішкі топтар:

$H_1=\{e, ab, ba^2\}$ $\quad$ $H_5=\{e, ab, ba^2\}$

$H_2=\{e, a, a^2\}$ $\quad$ $H_6=\{e, a^2b, ba\}$

$H_3=\{e, b\}$ $\quad$ $H_7=\{e, a^2ba\}$

$H_4=\{e, bab, aba\}$ $\quad$ $H_8=\{e, aba^2\}$

Кері элементтер:

$(e)^{-1} = e$ $(a^2ba)^{-1} = a^2ba$

$(a^2)^{-1} = a$ $(aba^2)^{-1} = aba^2$

$(ba^2)^{-1} = ab$ $(a)^{-1} = a^2$

$(a^2b)^{-1} = ba$ $(bab)^{-1} = aba$

$(aba)^{-1} = bab$ $(ab)^{-1} = ba^2$

$(b)^{-1} = b$ $(ba)^{-1} = a^2b$

$\overset{\equiv}{c}$- түйіндес қатынасының нышаны

$(a_r \equiv b) \overset{def}{\Leftrightarrow} (\exists x \in G)(a^x = b)$

3 кесте – T_{12}-ші топ элементтер түйіндесінің кестесі

*	e	a	ab	ba	bab	b	a^2ba	aba^2	a^2	aba	ba^2	a^2b
e	e	e	e	e	e	e	e	e	e	e	e	e
a	a	a	bab	ab	ba	bab	ab	ba	a	ab	ba	bab
ab	ab	ba	ab	bab	a	ba	a	bab	bab	ba	ab	a
ba	ba	bab	a	ba	ab	ab	bab	a	ab	a	bab	ba
bab	bab	ab	ba	a	bab	a	ba	ab	ba	bab	a	ab
b	b	a^2ba	a^2ba	a^2ba	a^2ba	b	b	b	aba^2	aba^2	aba^2	aba^2
a^2ba	a^2ba	aba^2	aba^2	aba^2	aba^2	a^2ba	a^2ba	a^2ba	b	b	b	b
aba^2	aba^2	b	b	b	b	aba^2	aba^2	aba^2	a^2ba	a^2ba	a^2ba	a^2ba
a^2	a^2	a^2	aba	ba^2	a^2b	aba	ba^2	a^2b	a^2	ba^2	a^2b	aba
aba	aba	ba^2	a^2b	a^2	aba	a^2	a^2b	ba^2	a^2b	aba	a^2	ba^2
ba^2	ba^2	a^2b	ba^2	aba	a^2	a^2b	a^2	aba	aba	a^2b	ba^2	a^2
a^2b	a^2b	aba	a^2	a^2b	ba^2	ba^2	aba	a^2	ba^2	a^2	aba	a^2b

Топ түйіндес элементтерінің кластары T_{12}:

$\overset{c}{e} = \{e\}$. $\overset{c}{a} = \{a, bab, ab, ba\}$. $\overset{c}{ab} = \{a, bab, ab, ba\}$.

$\overset{c}{ba} = \{a, bab, ab, ba\}$. $\overset{c}{bab} = \{a, bab, ab, ba\}$. $\overset{c}{b} = \{b, a^2ba, aba^2\}$.

$\overset{c}{a^2ba} = \{b, a^2ba, aba^2\}$. $\overset{c}{aba^2} = \{b, a^2ba, aba^2\}$. $\overset{c}{a^2} = \{a^2, a^2b, ba^2, aba\}$.

$\overset{c}{aba} = \{a^2, a^2b, ba^2, aba\}$. $\overset{c}{ba^2} = \{a^2, a^2b, ba^2, aba\}$. $\overset{c}{a^2b} = \{a^2, a^2b, ba^2, aba\}$.

Қорытындысында төрт әр түрлі T_{12} тобының түйіндес элементтер класы болады.

Граф төбелері үшін түйіндес элементтер кластарынан алынған элементтерді, ал граф қабырғалары үшін централизаторлы-эквивалентті элементтер класының элементтерін аламыз. Құрылған графтар тетраэдрлар тобының түйіндес элементтерінің әрбір көрнекі класын береді. Графтар ілмегі – бұл төбедегі элементті орынында қалдыратын элементтер, яғни граф төбелері элементтерінің централизаторы. Берілген түйіндес элементтер класында қанша элементтер болса, графтың әрбір төбесінен сонша қабырғалар шығады. Тетраэдрлар тобы төрт графтан тұратынын айта кетсек, оның ішінде екеуі төбелерінің саны мен құрылымы бойынша ұқсас болады.

Айтылған графтардың түйіндес элементтер кластарында өзара кері элементтер бар, сонымен қоса бұл элементтер тақ ретті болады. Сонымен қатар төбелері b болатын граф топта жалғыз, ал төбе болатын әрбір элемент екінші ретті болады.

1 - $e,a,a^2,b,ab,ba,a^2b,ba^2,$
aba,bab,a^2ba,aba^2

2 - e,a,a^2

3 – e,ab,ba^2

4 – a,ba,a^2b

5 – e,aba,bab

6 – a,a^2ba,ba

7 – a^2,ab,a^2ba

8 – bab,aba^2,ba

9 – b,ab,aba

10 – a^2b,bab,a^2ba

11 – ba,ba^2,aba

12 – a^2ba,aba^2

13 – a^2b,aba^2,a

14 – b,ba,ba^2

15 – b,ab,a^2b

16 – a,b,aba

17 – a^2,b,bab

27 - e,a,a^2

28 – e,ab,ba^2

29 – a,ba,a^2b

30 – e,aba,bab

31 – a,ba^2,a^2ba

32 – a^2,ab,a^2ba

33 – b,ab,a^2b

34 – b,ba,ba^2

35 - a^2b,a^2ba,bab

36 – ba,aba,a^2ba

37 – a,b,aba

38 – a^2,b,ba^2

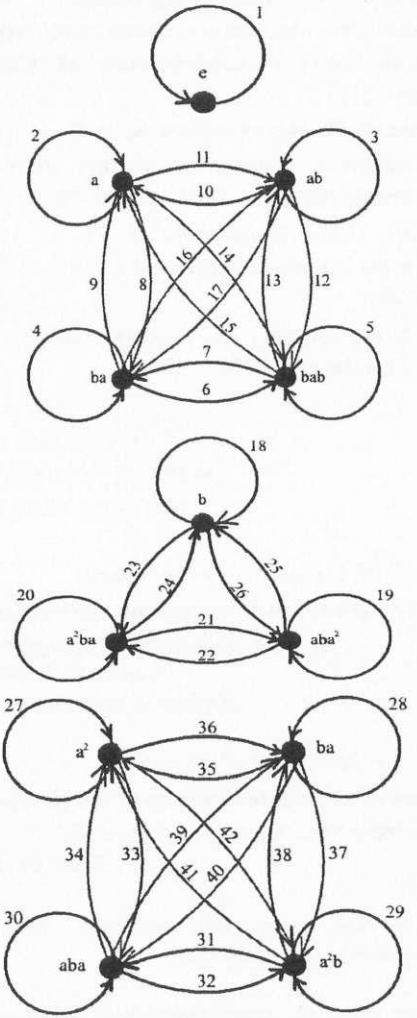
39 – a,a^2b,aba^2

40 – a^2,ba,aba^2

41 – ba^2,bab,aba^2

42 – ab,aba^2,aba

Тетраэдрлар тобаның түйіндес элементтер класының графын құрастырайық:



1 сурет – Тетраэдр тобының түйіндес элементтер класының бағандары

ӘДЕБИЕТТЕР ТІЗІМІ

1 **Павлюк, И. И., Пирожкова, Ю.Р.** Отношения эквивалентности на элементах конечных групп.// Материалы республиканской научной конференции «4 Сатпаевские чтения». – 2004. – С. 118-121.

2 **Павлюк, И.И., Султанбекова, А.Е.** О графовой структуре классов сопряжённых элементов групп.// «Вестник ПГУ» серия физико-математическая №2. – 2005. – С. 68-72.

3 **Павлюк, И.И., Жулдасов, Ж.М.** О графовой структуре группы нечетного порядка Вестник ПГУ им. С.Торайгырова» №4, – 2006. – С. 37-48.

4 **Магнус, В., Каррас, А., Солитер, Д.** Комбинаторная теория групп. – Москва: «Наука», 1974. – 460 с.

С. Торайғыров атындағы Павлодар
мемлекеттік университеті, Павлодар қ.
Материал 12.06.13 редакцияға түсті.

В. О. Будкова, И. И. Павлюк, А. Ф. Зейнулина

Граф классов сопряженных элементов группы тетраэдра

Павлодарский государственный университет
имени С. Торайгырова, Павлодар.
Материал поступил в редакцию 12.06.13.

V. O. Budkova, I. I. Pavlyuk, A. F. Zeynulina

Graph of classes of conjugate elements of the group of the tetrahedron

Pavlodar State University named after S. Toraigyrov, Pavlodar.
Material received on 12.06.13.

В работе дано представление группы тетраэдра графами классов сопряженных элементов.

The study gives the representation of the group of tetrahedron graphs of classes of conjugate elements

УДК 512.774.3

Б. Н. Дроботун, Н. И. Мухамедзянова, Е. Ш. Оралов

К ВОПРОСУ ПРОПЕДЕВТИЧЕСКОГО ИЗУЧЕНИЯ ОТНОШЕНИЯ ИЗОМОРФИЗМА И АБСТРАКТНЫХ СВОЙСТВ АЛГЕБРАИЧЕСКИХ СИСТЕМ (II)

В работе предлагаются технологические подходы к разработке примеров, способствующих формированию знаниевых схем применения метода от абстракции, как одного из основных методов математического познания, на основе реализации возможностей канонического перехода от квазиупорядоченных структур к частично (линейно) упорядоченным структурам.

В данной работе, являющейся непосредственным продолжением работ [1,2], авторы предлагают технологические подходы к построению примеров, способствующих формированию когнитивных схем применения метода от абстракции, как одного из основных методов математики. Формальной основой применения метода от абстракции послужила возможность канонического перехода от квазиупорядоченного множества к частичному (линейному) порядку на множестве классов некоторого разбиения этого множества, т.е. к ному отношению на множестве элементов новой природы.

Теорема 1 (теорема о переходе [3]). Пусть P – отношение квазипорядка на множестве M. Тогда:

а) бинарное отношение $\sim_P$; определённое на M по правилу:

$$(\forall x \in M)(\forall y \in M)((x \sim_P y) \Leftrightarrow ((xPy) \,\&\, (yPx)))$$

является отношением эквивалентности на множестве M;

б) бинарное отношение P^*, определённое на фактор-множестве $M/\sim_P$ по правилу:

$$(\forall [x]_{\sim_P} \in M/\sim_P)(\forall [y]_{\sim_P} \in M/\sim_P)(([x]_{\sim_P} P^* [y]_{\sim_P}) \Leftrightarrow$$

$$\Leftrightarrow ((\exists x' \in [x]_{\sim_P})(\exists y' \in [y]_{\sim_P})(x'Py')))$$

является отношением частичного порядка.

Канонический гомоморфизм $\varepsilon : \langle M; P\rangle \to \langle M/\sim_P; P^*\rangle$, определённый (в терминологии и символике этой теоремы) по правилу $(\forall x \in M)(\varepsilon(x) = [x]_{\sim_P})$, в случаях конкретных квазиупорядоченных множеств, лежит в основе введения новых понятий «методом от абстракции».

Формальная реализация «метода от абстракции», в данном случае, осуществляется по следующей схеме.

1) Отношение P теоремы о переходе может рассматриваться как отношение, полученное посредством проведения сравнительного анализа элементов множества M, с целью выявления свойства (характеристического признака), которым могут обладать элементы этого множества и который, в соответствии с задачами исследования, может быть положен в основу их классификации.

2) «Отождествление» различных в общем случае, но одинаково устроенных с позиций выявленного признака, объектов приводит к отношению эквивалентности на множестве M (отношение $\sim_P$ теоремы о переходе).

3) Полученное бинарное отношение P, как отношение на объектах данного множества M, естественным образом переносится на отношение между классами отождествлённых объектов, т. е. на отношение между элементами новой природы – элементами фактор-множества $M/\sim_P$ (отношение P^* теоремы о переходе и канонический гомоморфизм ε).

4) Переход от отношения P^* к характеризации элементов фактор-множества $M/\sim_P$ «по модулю» выделенного свойства (или совокупности свойств) приводит к выявлению содержания и объёма нового понятия.

В связи с этой теоремой сделаем следующие замечания:

Замечание 1. Переход от квазипорядка P на множестве M к частичному порядку P^* на фактор-множестве $M/\sim_P$, есть переход от $M;P$ к фактор-модели $M/\sim_P; P^*$, при этом, отношение P^* определяется на $M/\sim_P$ в соответствии с общей методологией построения фактор-модели в общей теории алгебраических систем.

Замечание 2. Отношение P^* является связным тогда и только тогда, когда исходное отношение P – связно (таким образом, в случае связного квазипорядка P, отношение P^* будет не только частичным, но и линейным порядком).

Понятийно-терминологическая база и символика данной статьи согласованы с терминологией и системой символических обозначений работ [4;5].

Продемонстрируем технологии применения метода от абстракции на конкретных примерах.

Пример 1. Пусть M={{7;8}; {3;12}; {10;6}; {4;9}; {4;15}; {3;8}; {18;2}} и P – бинарное отношение, определенное на множестве M следующим условием:

$(\forall\{a,b\} \in M)(\forall\{c,d\} \in M)(\{a,b\}P\{c,d\}) \Leftrightarrow$ (площадь прямоугольного треугольника с катетами a и b не превосходит площади прямоугольного треугольника с катетами c и d)). (1)

1) Выпишем элементы отношения P, как подмножества декартова квадрата M^2 множества M.

2) Докажем, что P - отношение связного квазипорядка.

3) Перейдем, основываясь на теореме о переходе, от этого отношения к отношению эквивалентности $\sim_P$ на множестве M и найдем фактор-множество $M/\sim_P$.

4) Построим граф $G_{\sim_P}$ и найдем характеристическую матрицу $M_{\sim_P}$ этого отношения.

5) Определим, следуя теореме о переходе, отношение линейного порядка P^* на фактор-множестве $M/\sim_P$, найдем матрицу M_{P^*} этого отношения и геометрическое представление графа G_{P^*} линейно упорядоченного множества

$M/\sim_P = \langle M/\sim_P ; P^* \rangle$.

1) Для удобства выписывания отношения P^*, как подмножества множества M^2, построим таблицу, в первой строке которой даны элементы множества M, т.е. длины катетов, а во второй – площади соответствующих прямоугольных треугольников (смотри таблицу 1).

Таблица 1 – Исходные данные

$\{a;b\}$	{7;8}	{3;12}	{10;6}	{4;9}	{4;15}	{3;8}	{18;2}
Площадь	28	18	30	18	30	12	18

Исходя из правила (1) определения отношения P и таблицы 1, получаем:

P ={({7;8};{7;8}); ({3;12};{3;12}); ({10;6};{10;6}); ({4;9};{4;9}); ({4;15};{4;15});({3;8};{3;8});({18;2};{18;2});({7;8};{10;6});({7;8};{4;15}); ({3;12};{7;8});({3;12};{10;6});({3;12};{4;9});({3;12};{4;15});({3;12}; {18;2});({10;6};{4;15});({4;9};{7;8});({4;9};{3;12});({4;9};{10;6}); ({4;9};{4;15});({4;9};{18;2});({4;15};{10;6});({3;8};{7;8});({3;8};{3;12}); ({3;8};{10;6});({3;8};{4;9});({3;8};{4;15});({3;8};{18;2});({18;2};{7;8}); ({18;2};{3;12});({18;2};{10;6}); ({18;2};{4;9}); ({18;2};{4;15})}.

2) Для доказательства того, что бинарное отношение P является отношением связного квазипорядка, найдем, используя его поэлементную запись, характеристическую матрицу M_P этого отношения:

$$M_P = \begin{array}{c} \begin{matrix} \{7;8\} & \{3;12\} & \{10;6\} & \{4;9\} & \{4;15\} & \{3;8\} & \{18;2\} \end{matrix} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \end{array} \begin{matrix} \{7;8\} \\ \{3;12\} \\ \{10;6\} \\ \{4;9\} \\ \{4;15\} \\ \{3;8\} \\ \{18;2\} \end{matrix}$$

По матрице M_P проверим, используя критерии, полученные в работе [1], что это бинарное отношение P является рефлексивным, транзитивным и связным.

Действительно:

– все элементы главной диагонали матрицы M_P равны 1, т.е. отношение P рефлексивно;

– для доказательства транзитивности этого соотношения проверим выполнение условия

$$(M_P \& M_{(P \circ P)} = M_{(P \circ P)}. \qquad (2)$$

Вычислим матрицу $M_{(P\circ P)}$. Находя непосредственно результат «логического» произведения матрицы M_P на M_P, будем иметь: $M_{(P\circ P)} = M_P \circ M_P = M(P)$.

Отсюда $(M_P \& M_{(P\circ P)}) = (M_P \& M_P) = M_P = M_{(P\circ P)}$.

Выполнимость для отношения P условия (2) говорит о том, что это отношение является транзитивным;

– вычисляя матрицу $M_P \vee M_{P^{-1}}$, последовательно находим, соответственно, матрицы $M_1 = M_{P^{-1}}$ и $M_2 = M_P \vee M_{P^{-1}}$

$$M_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}; \; M_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \vee$$

$$\vee \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Т.к. все элементы матрицы $M_P \vee M_{P^{-1}}$, стоящие на местах вне главной диагонали, равны 1, то отношение P связно. Таким образом, отношение P действительно является отношением связного квазипорядка.

3) Согласно теореме о переходе, элементы $\{a; b\}$ и $\{c; d\}$ множества M будут находиться в отношении $\sim_P$ тогда и только тогда, когда $\{a, b\}P\{c, d\}$ и $\{c, d\}P\{a, b\}$. Применительно к нашему примеру, с учетом правила, определяющего бинарное отношение P, это означает, что

$$(\{a, b\} \sim_P \{c, d\}) \Leftrightarrow \left(\left(\frac{a\cdot b}{2} \le \frac{c\cdot d}{2}\right) \& \left(\frac{c\cdot d}{2} \le \frac{a\cdot b}{2}\right)\right) \Leftrightarrow \left(\frac{a\cdot b}{2} = \frac{c\cdot d}{2}\right) \quad (3)$$

Таким образом, в соответствии последним звеном цепочки эквивалентностей (3), элементы $\{a; b\}$ и $\{c; d\}$ множества M будут находиться в одном и том же классе эквивалентности (по отношению к $\sim_P$) тогда и только тогда, когда площади треугольников с катетами

a, b и c, d, соответственно, будут равны. Отсюда следует, что число классов эквивалентности множества M по отношению $\sim_P$ равно числу различных значений площадей прямоугольных треугольников с катетами a, b по всем элементам $\{a, b\} \in M$.

Исходя из таблицы 1 получаем, что число классов эквивалентности равно четырем, при этом:

– в первый класс входят такие элементы множества M, которым соответствуют прямоугольные треугольники с площадью 28;

– во второй – с площадью 18;

– в третий – с площадью 30;

– в четвертый – с площадью 12.

Отсюда следует, что разбиение множества M, соответствующее отношению $\sim_P$ и фактор-множество $M/\sim_P$ будет иметь следующий вид:

$$M = \{\{7; 8\}\} \cup \{\{3; 12\}; \{4; 9\}; \{18; 2\}\} \cup \{\{10; 6\}; \{4; 15\}\} \cup \{\{3; 8\}\}; \quad (4)$$

$$M/\sim_P = \{[\{7; 8\}]_{\sim_P}; [\{3; 12\}]_{\sim_P}; [\{10; 6\}]_{\sim_P}; [\{3; 8\}]_{\sim_P}\}. \quad (5)$$

Т.к. всякий класс эквивалентности порождается любым своим элементом, то равенство (5) идентично равенству

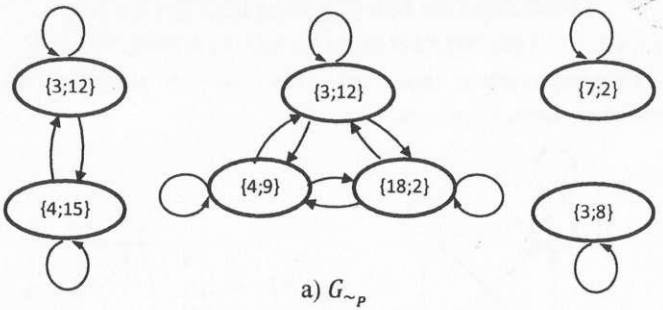
$$M/\sim_P = \{[\{7; 8\}]_{\sim_P}; [\{4; 9\}]_{\sim_P}; [\{4; 15\}]_{\sim_P}; [\{3; 8\}]_{\sim_P}\}. \quad (6)$$

Сопоставляя каждому классу площадь прямоугольного треугольника, соответствующего всем элементам из этого класса, можно считать, что фактор-множество $M/\sim_P$ с точностью до биективности, совпадает с множеством $\{28; 18; 30; 12\}$.

4) Т.к. элементы любого класса разбиения (4) попарно находятся в отношении $\sim_P$, то, исходя из этого разбиения, будем иметь:

$\sim_P = \{(\{7; 8\}; \{78\}); (\{3; 12\}; \{3; 12\}); (\{4; 9\}; \{4; 9\});$
$(\{18; 2\}; \{18; 2\}); (\{3; 12\}; \{4; 9\}); (\{4; 9\}; \{3; 12\}); (\{3; 12\}; \{18; 2\});$
$(\{18; 2\}; \{3; 12\}); (\{4; 9\}; \{18; 2\}); (\{4; 9\}; \{18; 2\}); (\{10; 6\}; \{10; 6\});$
$(\{4; 15\}; \{4; 15\}); (\{10; 6\}; \{4; 15\}); (\{4; 15\}; \{10; 6\}); (\{3; 8\}; \{3; 8\})\}$.

По отношению $\sim_P$, как подмножеству декартова квадрата M^2 множества M, получаем геометрическое представление $G_{\sim_P}$ графа этого отношения и строим его характеристическую матрицу $M_{\sim_P}$ (смотри рисунок 1. а), б)).



а) $G_{\sim_P}$

$$M_{\sim_P} = \begin{array}{c} \begin{matrix} \{7;8\} & \{3;12\} & \{4;9\} & \{18;2\} & \{10;6\} & \{4;15\} & \{3;8\} \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array} \begin{matrix} \{7;8\} \\ \{3;12\} \\ \{4;9\} \\ \{18;2\} \\ \{10;6\} \\ \{4;15\} \\ \{3;8\} \end{matrix}$$

б) $M_{\sim_P}$

Рисунок 1 – Граф $G_{\sim_P}$ и матрица $M_{\sim_P}$

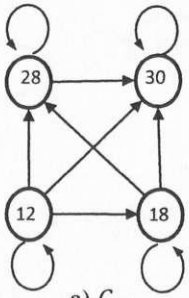
5) В пункте 3 рассматриваемого примера было показано, что бинарное отношение P является отношением связного квазипорядка. Следовательно, отношение P^*, в соответствии с теоремой о переходе, (смотри замечание 2) должно быть отношением линейного порядка.

Т.к. сравнение классов эквивалентности, как элементов новой природы из фактор-множества $M/\sim_P$, по отношению P^* осуществляется посредством сравнения по отношению P некоторых представителей из этих классов, т. е. (применительно к нашему примеру) посредством сравнения по величине площадей прямоугольных треугольников, соответствующих выбранным представителям, то бинарное отношение P^* на фактор-множестве $M/\sim_P$ совпадает с отношением $\leq$ (меньше или равно) на множестве {28;18; 30; 12}. Таким образом, линейно упорядоченные множества

$\boldsymbol{M/\sim_P} = \langle M/\sim_P; P^* \rangle$; и $\boldsymbol{S} = \langle S; \leq \rangle = \langle \{28;\ 18;\ 30;\ 12\}; \leq \rangle$ отличаются только природой элементов основных множеств, т.е. являются изоморфными. Поэтому отношение P^* с точностью до изоморфизма, может быть представлено следующим образом:

$P^* = \{(28;28);(18;18);(30;30);(12;12);(28;30);$
$(18;28);(18;30);(12;28);(12;18);(12;30)\}.$

Геометрическое представление G_{P^*} и матрица M_{P^*} этого отношения даны на рисунке 2 а), б).



а) G_{P^*}

$$M_{P^*} = \begin{array}{c} \\ 28 \\ 18 \\ 30 \\ 12 \end{array} \begin{array}{c} \begin{array}{cccc} 28 & 18 & 30 & 12 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

б) M_{P^*}

Рисунок 2 – Граф G_{P^*} и матрица M_{P^*}

Утверждение о том, что отношение P^*, полученное в нашем примере, является отношением линейного порядка, можно доказать и непосредственно, исходя из характеристической матрицы M_{P^*}.

Для этого, используя соответствующие критерии (смотри [1]), покажем, что отношение P^* рефлексивно, антисимметрично, транзитивно и связно. В самом деле:

– P^* является рефлексивным отношением, т.к. все элементы главной диагонали матрицы M_{P^*} равны 1;

– для подтверждения того, что это отношение антисимметричности, найдем матрицу $M_{P^* \cap (P^*)^{-1}}$ и убедимся в том, что все ее элементы, стоящие на местах вне главной диагонали, равны 0. Действительно, полагая $M_1 = M_{P^*} \& M_{(P^*)^{-1}}$, получим

$$M_{(P^*)^{-1}} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

$$M_1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \& \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

проверим, что матрица M_{P^*} удовлетворяет условию:

$M_{P^*} \& M_{P^* \circ P^*} = M_{P^* \circ P^*}$. (6)

Последовательно вычисляя матрицу $M_{P^*} \& M_{P^* \circ P^*}$, будем иметь:

$$M_{P^* \circ P^*} = M_{P^*} \circ M_{P^*} =$$

$$= \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} = M_{P^*}$$

Т.к. $M_{P^* \circ P^*} = M_{P^*}$, то $M_{P^*} \& M_{P^* \circ P^*} = M_{P^*} \& M_{P^*} = M_{P^*}$.

Выполнимость условия (6) для отношения P^* подтверждает его антисимметричность;

– для подтверждения того, что отношение P^* связно, достаточно убедится в том, что все элементы матрицы $\widehat{M} = M_{P^*} \vee M_{(P^*)^{-1}}$, занимающие места вне главной диагонали, равны 1.

Действительно:

$$\widehat{M} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \vee \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

В теореме о переходе подчеркивалось (смотри замечание 3), что если исходное отношение P являлось отношением связного квазипорядка, то отношение P^* будет не только частичным, но и линейным порядком.

В связи с этим, уместно отметить, что матрица M_{P^*} может быть получена из матрицы M_P удалением 4-ой, 5-ой и 7-ой строк и 4-го, 5-го и 7-го столбцов. Отмеченное положение является следствием того, что в качестве представителей из классов эквивалентности 28; 18; 30; 12 фактор-множества $M/\sim_P$ могут быть выбраны элементы {7;8};{3;12}; {10;6}; {3;8} (смотри равенство (5)), т.е. 1-ый, 2-ой, 3-ой и 6-ой элементы множества M, в порядке их записи в этом множестве. Аналогичным образом, матрица M_{P^*} может быть получена из матрицы M_P удалением 2-ой, 3-ей и 7-ой строк и 2- го, 3-го и 7- го столбцов, что также обусловлено возможностью другого выбора представителей из тех же классов эквивалентности, а именно – выбора элементов {7;8};{4;9}; {4;15}; {3;8} (смотри равенство (6)). Т.е., в любом случае, для получения матрицы M_{P^*} из матрицы M_P удаляются повторяющиеся строки и столбцы.

А т.к. проверка свойств рефлексивности, транзитивности и связности бинарных отношений, осуществляемая методами, основывающимися на алгоритмах оперирования с характеристическими матрицами, требует или поэлементного сравнения, или осуществляется поэлементным выполнением операции $\vee$, или выполнения операции $\circ$ – логического умножения, с последующим поэлементным выполнения операции &, то применение этих алгоритмов к исходной матрице M_P и матрице M_{P^*}, полученной из нее удалением повторяющихся строк и столбцов (с теми же номерами), приводят к одним и тем же выводам относительно вышеупомянутых свойств бинарных отношений P и P^*, представляемых этими матрицами.

Таким образом, утверждение, сделанное в замечании 2. к теореме о переходе получает красноречивое подтверждение «на языке» характеристических матриц.

Рассмотренный выше пример допускает следующее обобщение.

Пример 2. В качестве множества M, фигурирующего в этом примере, можно взять множество $\widehat{M}$ всех двухэлементных подмножеств множества R^+ – всех неотрицательных действительных чисел, т.е. полагать, что

$$\widehat{M} = \{\{a;b\}/a;b \in R^+\}$$

Бинарное отношение $\hat{P}$ задается на этом множестве по тому же правилу, что и отношение P в этом примере.

В связи с бесконечностью множества $\widehat{M}$ непосредственное поэлементное выписывание отношения $\hat{P}$, естественно, не может быть осуществлено.

По этой же причине невозможно задать это отношение посредством характеристической матрицы и графа. Все остальные рассуждения, а также построения (фигурирующие в теореме о переходе), касающиеся отношений P, $\sim_P$, P^* и их свойств, переносятся на отношения $\hat{P}$, $\sim_{\hat{P}}$, $\hat{P}^*$ практически без изменений.

В частности, использование общей схемы описания фактор-множеств с точностью до биективности применительно к фактор-множеству $M/\sim_P$ осуществляется так:

1) Определяющим признаком принадлежности элементов множества $\widehat{M}$ одному и тому же классу эквивалентности по отношению $\sim_{\hat{P}}$ является следующее положение: элементы $\{a; b\}$ и $\{c; d\}$ лежат в одном и том же классе эквивалентности тогда и только тогда, когда площади прямоугольных треугольников с катетами a, b и c, d, соответственно, совпадают;

2) В роли характеристики любого конкретного класса эквивалентности $[\{a, b\}]_{\sim_{\hat{P}}}$ будет выступать площадь $S_{\{a;b\}}$ прямоугольного треугольника с катетами a и b. Очевидно, что величина $S_{\{a;b\}}$ не зависит от выбора представителя из класса $[\{a, b\}]_{\sim_{\hat{P}}}$ и может рассматриваться в качестве описания (имени) всего этого класса, как элемента новой природы;

3) Убедившись в том, что для каждого действительного числа $S \in R^+$ существуют прямоугольные треугольники, площади которых равны S, и отождествляя классы эквивалентности $[\{a, b\}]_{\sim_{\hat{P}}}$ с их именами $S_{\{a;b\}}$, можно считать, что фактор-множество $\widehat{M}/\sim_P$ с точностью до биективности совпадает с множеством R^+, а линейно упорядоченное множество $\widehat{\boldsymbol{M}}/\sim_{\hat{P}} = \langle \widehat{M}/\sim_{\hat{P}}; \hat{P}^* \rangle$ с точностью до изоморфизма совпадает с линейно упорядоченным множеством $\boldsymbol{R}^+ = \langle R^+; \leq \rangle$. Формальное доказательство того, что $\widehat{\boldsymbol{M}}/\sim_{\hat{P}} \cong \boldsymbol{R}^+$ будет проверено ниже.

Если теперь определить отображение Φ: $\widehat{M} \to R$ по правилу:

$$(\forall \{a, b\} \in \widehat{M})(\Phi([a, b]) = S_{\{a;b\}}) \qquad (7)$$

то, исходя из вышеприведенного описания 1) – 3) фактор-множества $\widehat{M}/\sim_{\hat{P}}$, нетрудно получить композиционное представление этого отображения в виде:

$$\Phi = \varepsilon_{P_\Phi} \circ \tau \circ l_{Im\Phi}. \qquad (8)$$

Предварительно заметим, что:

а) $Im\Phi = R^+$;

б) $P_\Phi = \sim_{\hat{P}}$.

Конкретизируя общие определения композиционных «сомножителей» из теоремы о представлении отображений

применительно к конкретному отображению Φ, определенному по правилу (7), получаем, что отображение ε_{P_Φ}:τ и l_{Im_Φ} (смотри [1]) задаются, соответственно, по следующим правилам:

$$(\forall \{a,b\} \in \widehat{M})(\varepsilon_{P_\Phi}(\{a,b\}) = [\{a,\ b\}]_{P_\Phi}); \quad (9)$$

$$\left(\forall [\{a,b\}]_{P_\Phi} \in \widehat{M}/{\sim_{\hat{P}}}\right) = (\tau([\{a,\ b\}]_{P_\Phi}) = S_{\{a;b\}}); \quad (10)$$

$$(\forall\, c \in R^+)(l_{Im_\Phi}(c) = c). \quad (11)$$

Таким образом, в соответствии с правилами (9), (10), (11):

– посредством сюръекции $\varepsilon_{P_\Phi}: \widehat{M} \to \widehat{M}/P_\Phi$ элемент $\{a,b\}$ отображается в класс эквивалентности $[\{a,\ b\}]_{P_\Phi}$, порожденный этим элементом, т.е., как отмечалось ранее, в класс всех прямоугольных треугольников, имеющих одну и ту же площадь, равную $\frac{a \cdot b}{2}$ (смотри правило (9));

– посредством биекциит: $\widehat{M}/{\sim_{P_\Phi}} \to R^+$ классу $[\{a,\ b\}]_{\sim_{P_\Phi}}$ ставится в соответствие площадь $S_{\{a;b\}}$ прямоугольного треугольника с катетами a и b, т.е. имя этого класса (смотри правило (10));

– посредством инъекции $l_{Im_\Phi}: R^+ \to R$ числовое выражение $S_{\{a;b\}} = c$ – площади, как величины, имеющей определенную размерность, отображается в действительное неотрицательное число c, как величину безразмерную (смотри правило (11)).

Напомним, что отношение $\hat{P}$ определяется на множестве $\widehat{M}$ по правилу, аналогичному правилу (1), т.е.

$$\left(\forall \{a,b\} \in \widehat{M}\right)\left(\forall \{c,d\} \in \widehat{M}\right)\left(\left(\{a,b\}\hat{P}\{c,d\}\right) \Leftrightarrow \left(S_{\{a;b\}} \le S_{\{c,d\}}\right)\right) \quad (12)$$

Согласно определению (7) отображения Φ, имеем:

$S_{\{a;b\}} = \ = \Phi(\{a,b\})$, $S_{\{c;d\}} = \Phi(\{c,d\})$. Отсюда получаем, что

$$\left(S_{\{a;b\}} \le S_{\{c,d\}}\right) \Leftrightarrow (\Phi(\{a,b\}) \le \Phi(\{c,d\})) \quad (13)$$

Из (12) и (13) следует, что

$$\left(\forall \{a,b\} \in \widehat{M}\right)\left(\forall \{c,d\} \in \widehat{M}\right)\left(\left(\{a,b\}\hat{P}\{c,d\}\right) \Leftrightarrow\right.$$

$$\left.\Leftrightarrow (\Phi(\{a,b\}) \le \Phi(\{c,d\}))\right). \quad (14)$$

Заметим, что множества $\widehat{M}$ и R вместе с определенными на них бинарными отношениями $\hat{P}$ и $\le$, т.е. двуместными предикатами, соответственно, можно рассматривать как модели $\langle \widehat{M}; \hat{P} \rangle$ и $\langle R; \le \rangle$.

Из соотношения (14) следует, что отображение $\Phi: \widehat{M} \to R$ является строгим (а значит и сильным) гомоморфизмом модели $\widehat{\boldsymbol{M}} = \langle \widehat{M}; \hat{P} \rangle$ в модель $\boldsymbol{R} = \langle R; \leq \rangle$.

Отсюда, по теореме о гомоморфизмах алгебраических систем, получаем, что

$\langle \widehat{M}/\sim_{\hat{P}}; \hat{P}^* \rangle = \widehat{\boldsymbol{M}}/\sim_{\hat{P}} \cong \boldsymbol{Im\Phi} = \langle Im\Phi; \leq \rangle$.

А так как $Im\Phi = R$, то линейно упорядоченные множества $\langle \widehat{M}/\sim_{\hat{P}}; \hat{P}^* \rangle$ и $\langle R^+; \leq \rangle$ действительно изоморфны.

СПИСОК ЛИТЕРАТУРЫ

1 **Дроботун, Б. Н., Мухамедзянова, Н. И., Оралов, Е. Ш.** Отношение изоморфизма и абстрактные свойства алгебраических систем (I). – Павлодар: Изд-во ПГУ, Наука и техника Казахстана, 2012. – №1.

2 **Дроботун, Б. Н., Мухамедзянова, Н. И., Оралов, Е. Ш.** К вопросу пропедевтического изучения отношения изоморфизма и абстрактных свойств алгебраических систем (I). – Павлодар: Изд-во ПГУ, Наука и техника Казахстана, 2012. – №1.

3 **Гончаров С. С., Дроботун Б. Н., Никитин А. А.** Методические аспекты изучения алгебраических систем в высшем учебном заведении: Моногр. – Новосибирск: Изд-во НГУ, 2007. – 250 с.

4 **Мальцев, А. И.** Алгебраические системы. – М.: Наука, 1970. –392 с.

5 **Ершов, Ю. Л., Палютин, Е. А.** Математическая логика. – М.: Наука, 1997. – 320 с.

Павлодарский государственный университет
имени С. Торайгырова, г. Павлодар.
Материал поступил в редакцию 29.04.13.

Б. Н. Дроботун, Н. И. Мухамедзянова, Е. Ш. Оралов

Алгебралық жүйенің абстрактілік құрылымын және изоморфизма қатынасын пропедевтикалық зерттеу мәселесі

С. Торайғыров атындағы
Павлодар мемлекеттік университеті, Павлодар қ.
Материал 29.04.13 редакцияға түсті.

B. N. Drobotun, N. I. Mukhamedzjanova, E. Sh. Oralov

On propaedeutic study of the relations of isomorphism and abstract properties of algebraic systems

Pavlodar State University named after S. Toraigyrov, Pavlodar.

Material received on 29.04.13.

Жұмыста математикалық танымдық негізгі әдістерінің бірі сияқты, абстракциядан, білім сұлбалары қалыптастыруды қамтамасыз ету, квазореттік құрылымнан ішінара (желілік, сызықтық) реттелген құрылымдарға каноникалық ауысу мүмкіндіктері жүзеге асыру негізінде қолдану әдісін мысалдарын жасауда технологиялық көзқарастар ұсынылады.

In work technological approaches to development of the examples promoting formation of knowledge schemes of application of a method from abstraction, as one of the main methods of mathematical knowledge, on the basis of realization of opportunities of initial transition from quasiordered structures to the partially (linearly) ordered structures are offered.

УДК 511.238

Б. Н. Дроботун, О. И. Панасенко

ГРУППЫ ГАЛУА И СООТВЕТСТВИЯ ГАЛУА КОНЕЧНЫХ РАСШИРЕНИЙ ПОЛЯ РАЦИОНАЛЬНЫХ ЧИСЕЛ (I)

В данной работе, посвященной разработке методологических подходов к изучению основ теории Галуа в высших учебных заведениях, дается описание технологий представления групп Галуа составных алгебраических расширений (степени 2) поля рациональных чисел посредством подгрупп группы подстановок.

1. Содержание классической теории Галуа связано с выявлением и реализацией возможностей применения методов теории групп к изучению конечных, сепарабельных и нормальных расширений $\mathcal{F}$ данного поля $\mathcal{P}$.

Автоморфизмы поля $\mathcal{F}$, оставляющие элементы подполя $\mathcal{P}$ неподвижными, т. е. автоморфизмы Φ, удовлетворяющие условию

$$(\forall x \in \mathcal{P})(\Phi(x) = x)$$

образуют группу относительно операции их последовательного выполнения. Эта группа называется группой Галуа расширения $\mathcal{F}$ поля $\mathcal{P}$ и будет обозначаться далее через $G\left(\mathcal{F}/\mathcal{P}\right)$.

Если $\mathcal{H}$ - произвольная подгруппа группы $G\left(\mathcal{F}/\mathcal{P}\right)$, то элементы поля $\mathcal{F}$, которые остаются неподвижными под действием всех автоморфизмов из подгруппы $\mathcal{H}$ образуют подполе $\mathcal{L}$ поля $\mathcal{F}$. Это неподвижное подполе является промежуточным между ролями $\mathcal{P}$ и $\mathcal{F}$, т. е. $\mathcal{P} \le \mathcal{L} \le \mathcal{F}$.

Основная терема теории Галуа [1] утверждает, что если подставить в соответствие каждой подгруппе $\mathcal{H}$ группы $G\left(\mathcal{F}/\mathcal{P}\right)$ ее неподвижные подполе $\mathcal{L}$, то полученное соответствие будет антиизоморфным

отображением решетки подгрупп группы $G\left(\mathcal{F}/\mathcal{P}\right)$ на решетку промежуточных подполей поля $\mathcal{F}$, заключенных между $\mathcal{P}$ и $\mathcal{F}$.

Э. Галуа, разрабатывая математический аппарат, предназначенный для получения критерия разрешимости алгебраических уравнений в радикалах, создал теорию (носящую в настоящее время его имя), непреходящее значение которой заключатся в выявлении и обосновании системообразующей роли групп симметрий математических объектов, как конкретных воплощениях общей идеи симметрии.

В рамках этой теории Э. Галуа были получены необходимые и достаточные условия разрешимости уравнений

$$a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n = 0\,,\ (a_i \in P\,,\ i = 1;2;...;n)\,,$$

в радикал т. е. условия, гарантирующие возможности представления корней этих уравнений через коэффициенты $a_0;a_1;...;a_{n-1};a_n$ посредством применения к ним арифметических операций (сложения, умножения, вычитания, деления) и извлечения корней определенных степеней (т. е. применения радикалов).

Как отмечается в [2] «…Применение теории Галуа к вопросу о разрешимости уравнений в радикалах осуществляется следующим образом. Пусть f - многочлен от x над полем $\mathcal{P}$, $\mathcal{F}$ - поле разложения этого многочлена и $G\left(\mathcal{F}/\mathcal{P}\right)$ - группа Галуа расширения $\mathcal{F}/\mathcal{P}$. Она называется группой многочлена f над полем $\mathcal{P}$ (ее элементы естественным образом изображаются подстановками корней уравнения $f(x)=0$). Оказывается, уравнение $f(x)=0$ тогда и только тогда решается в радикалах, когда группа Галуа многочлена f полициклическая" ([2], стр.11).

2. Если рассматривать в качестве данного поля $\mathcal{P}$ - простое поле характеристики 0, т. е. поле рациональных чисел, то каждое расширение этого поля будет сепарабельным. В этом случае изложение основ теории Галуа, не утрачивая своей идейно-методологической значимости, становится (в техническом отношении) несколько проще.

В данной статье, представляющей собой первую часть работы, посвященной выявлению технологических подходов к изучению основ теории Галуа в высших учебных заведениях, разрабатываются методы демонстрационного сопровождения базовых положений этой теории и возможностей применения ее средств к вопросам разрешимости уравнений $f\ x\ = 0\ \ (f\ x\ \in Q[x])$ в радикалах.

Описание предлагаемых технологий, данное применительно к расширению $\boldsymbol{Q}(\alpha_1;\alpha_2;\alpha_3)$, где $\alpha_1;\alpha_2;\alpha_3$ - алгебраические над полем $\boldsymbol{Q}$ элементы степени 2, аккумулирует в себе возможности обобщения получаемых результатов на случай присоединения к полю $\boldsymbol{Q}$ любого конечного числа алгебраических над этим полем элементов $\alpha_1;\alpha_2;\ldots;\alpha_t\ \ (t>3)$ степени 2.

Следует отметить, что в настоящее время базовая алгебраическая подготовка студентов высших учебных заведений, обучающихся по специальности «Математика», претерпев существенные сокращения, проводится на протяжении 1 семестра (3 кредита) в рамках учебной дисциплины «Основы алгебры». Таким образом, дальнейшее изучение алгебры, как фундаментальной составляющей естественно-математических наук, операционные возможности которой предопределили алгебраизацию современного математического языка, предполагается осуществлять средствами элективных дисциплин и специальных курсов логико-алгебраической направленности.

Результаты данной работы могли бы составить основу специального курса «Элементы теории Галуа», как спецкурса, завершающего формирование логико-алгебраической культуры студентов.

В работе используются общепринятые логико-алгебраическая терминология и система символических обозначений [1,2].

3. Пусть $\boldsymbol{F}=\left\langle F;+\ ;\cdot\ ;^{-1};-;0;1\right\rangle$ - поле и $\boldsymbol{P}=\left\langle P;+\ ;\cdot\ ;^{-1};-;0;1\right\rangle$ - его подполе. Поле $\boldsymbol{F}$, как расширение поля $\boldsymbol{P}$, можно считать векторным пространством $\left\langle F;+;\ {}^{w_\alpha}\!/_{\alpha\in P}\ ;0\right\rangle$ над этим полем. Здесь w_α - унарная операция, определенная на F по правилу $w_\alpha\ a=\alpha a$ для любых элементов $\alpha\in P$ и $a\in F$, т. е. операция «умножения» элементов a из F, которые берутся в качестве векторов, на элементы α из P, рассматриваемых, как скаляры.

Расширение $\mathcal{F}$ поля $\mathcal{P}$ называется конечным, если оно, как векторное пространство над $\mathcal{P}$, имеет конечную размерность. Размерность $\mathcal{F}$ над $\mathcal{P}$ обозначается через $[\mathcal{F}:\mathcal{P}]$.

Через $\mathcal{P}[x]$ обозначается кольцо многочленов от одной переменной x над полем $\mathcal{P}$, т. е. носитель $P[x]$ этого кольца есть множество всех многочленов от одной переменной x с коэффициентами из поля P.

Элемент $\alpha \in F$ называется алгебраическим над полем $\mathcal{P}$, если он является корнем некоторого многочлена ненулевой степени из $P[x]$. Если α - алгебраический над $\mathcal{P}$ элемент, то минимальным многочленом этого элемента называется нормированный многочлен наименьшей степени из $P[x]$, корнем которого является α. Степень этого минимального многочлена называется степенью элемента α.

Определение 1. Пусть $\mathcal{F}$ - поле, $\mathcal{P}$ - его подполе, $\alpha \in F$ и α алгебраический над $\mathcal{P}$ элемент. Простым алгебраическим расширением поля $\mathcal{P}$, посредством элемента α, называется наименьшее подполе поля $\mathcal{F}$, носитель которого содержит P и элемент α.

Полученное подполе обозначается далее через $\mathcal{P}(\alpha)$, при этом говорят, что поле $\mathcal{P}(\alpha)$ получается из поля $\mathcal{P}$ присоединением к нему алгебраического элемента α.

Одним из наиболее информативных описаний строения поля $\mathcal{P}(\alpha)$ является его описание в терминах векторных пространств [1].

Теорема 1. Пусть $\mathcal{F}$ - поле, $\mathcal{P}$ - его подполе и α - алгебраический над $\mathcal{P}$ элемент степени n. Тогда поле $\mathcal{P}(\alpha)$ является векторным пространством над полем $\mathcal{P}$ размерности n, при этом элементы

$$1;\alpha;\alpha^2;\ldots;\alpha^{n-1} \qquad (1)$$

составляют его базис.

В соответствии с теоремой 1, всякий элемент β поля $\mathcal{P}(\alpha)$ есть линейная комбинация элементов $1;\alpha;\alpha^2;\ldots;\alpha^{n-1}$ базиса (1) с коэффициентами из P. Другими словами β - есть значение многочлена $h(x) \in P[x]$, степень которого не превосходит $n-1$, при $x=\alpha$, т. е. $\beta = h(\alpha)$.

Определение 2. Расширение $\mathcal{F}$ поля $\mathcal{P}$ называется составным алгебраическим расширением, если существует возрастающая цепочка подполей $\mathcal{L}_i$ $(i=0;1;...;t)$ поля $\mathcal{F}$, таких что

$$\mathcal{P}=\mathcal{L}_0 \prec \mathcal{L}_1 \prec \ldots \prec \mathcal{L}_{t-1} \prec \mathcal{L}_t = \mathcal{F} \qquad (2)$$

и поле $\mathcal{L}_k$ является простым алгебраическим расширением поля

$$\mathcal{L}_{k-1} \ (k=1;2;...;t).$$

Длину t цепочки (2) будем называть порядком составного алгебраического расширения.

Таким образом если $\mathcal{F}$ - составное алгебраическое расширение поля $\mathcal{P}$ порядка t $(t>1)$, то существуют такие элементы $\alpha_1;\alpha_2;...;\alpha_t \in F$, что элемент α_1 является алгебраическим над $\mathcal{P}$ и элемент α_i является алгебраическим над полем $\mathcal{P}(\alpha_1;\alpha_2;...;\alpha_{i-1})$ для любого $i \in \{2;3;...;t\}$.

Теорема 2. Пусть $\mathcal{F}$ - составное алгебраическое расширение поля $\mathcal{P}$ порядка 2, т. е.

$$\mathcal{P}=\mathcal{P}(\alpha) \prec (\mathcal{P}(\alpha))(\beta)=\mathcal{F}, \qquad (3)$$

для некоторых элементов α и β, алгебраических над полями $\mathcal{P}$ и $\mathcal{P}(\alpha)$, соответственно. Тогда:

$$[\mathcal{F}:\mathcal{P}]=\left[\mathcal{P}(\alpha;\beta):\mathcal{P}(\alpha)\right]\cdot\left[\mathcal{P}(\alpha):\mathcal{P}\right];$$

если $\left[\mathcal{P}(\alpha;\beta):\mathcal{P}(\alpha)\right]=n, \left[\mathcal{P}(\alpha):\mathcal{P}\right]=m$, и $1;\alpha;\alpha^2;...;\alpha^{m-1}$ - базис поля $\mathcal{P}(\alpha)$ над $\mathcal{P}$, а $1;\beta;\beta^2;...;\beta^{n-1}$ базис поля $\mathcal{P}(\alpha;\beta)$ над $\mathcal{P}(\alpha)$, то $\left\{\alpha^i\beta^j \Big/ i=0;1;...;m-1;\ j=0;1;...;n-1\right\}$ - базис поля $\mathcal{P}(\alpha;\beta)$ над $\mathcal{P}$.

4. Возникает естественный вопрос, в каком случае составное алгебраическое расширение $\mathcal{F}=\mathcal{P}(\alpha_1;\alpha_2;...;\alpha_t)$, порядка $t>1$, поля $\mathcal{P}$ является простым, т. е. получается из $\mathcal{P}$ присоединением одного, так называемого, примитивного элемента θ. При условии существования такого элемента, будет иметь место равенство

$$\mathcal{P}(\alpha_1;\alpha_2;...;\alpha_t)=\mathcal{P}(\theta),$$

т. е. t – кратная процедура последовательного построения простых алгебраических расширений сведется к однократной.

Ответ на поставленный вопрос дает нижеследующая теорема [1]. Эта теорема сформулирована применительно к числовым полям, т. е. полям характеристики 0, т. к. при дальнейшем изложении работы роль поля $\mathcal{P}$ будет играть поле Q - рациональных чисел, а поле $\mathcal{F}$ будет некоторым подполем поля C - комплексных чисел.

Теорема 3 (теорема о примитивном элементе). Пусть числовое поле $\mathcal{F}$ является составным алгебраическим расширением поля $\mathcal{P}$ порядка $t > 1$, т. е.

$$\mathcal{P} = \mathcal{P}(\alpha_1) \prec \mathcal{P}(\alpha_1;\alpha_2) \prec \ldots \prec \mathcal{P}(\alpha_1;\alpha_2;\ldots;\alpha_t) = \mathcal{F},$$

для некоторых элементов $\alpha_1;\alpha_2;\ldots;\alpha_t \in F$ таких, что α_1 является алгебраическим над $\mathcal{P}$, а α_{t+1} - над $\mathcal{P}(\alpha_1;\alpha_2;\ldots;\alpha_t)$, и $\mathcal{P}(\alpha_1;\alpha_2;\ldots;\alpha_t) = \mathcal{F}$. Тогда существует элемент $\theta \in \mathcal{F}$ такой что $\mathcal{P}(\alpha_1;\alpha_2;\ldots;\alpha_t) = \mathcal{P}(\theta)$.

Нетрудно видеть, основываясь на соображениях индуктивного характера, что достаточно указать способ построения примитивного элемента для составных алгебраических расширений порядка 2.

Действительно, при наличии такого метода, построение примитивного элемента θ для составного алгебраического расширения $\mathcal{P}(\alpha_1;\alpha_2;\ldots;\alpha_t)$ при $t \geq 3$, может быть осуществлено индукцией по натуральному параметру t.

А именно, будем предполагать, что для любых, уловлетворяющих условию теоремы элементов $\beta_1;\beta_2;\ldots;\beta_k$ примитивный элемент θ' уже найден, т. е. $\mathcal{P}(\beta_1;\beta_2;\ldots;\beta_k) = \mathcal{P}(\theta)$. Тогда исходя из того, что

$$\mathcal{P}(\beta_1;\beta_2;\ldots;\beta_{k+1}) = (\mathcal{P}(\beta_1;\beta_2;\ldots;\beta_k)(\beta_{k+1})) = (\mathcal{P}(\theta'))(\beta_{k+1}) =$$
$$= \mathcal{P}(\theta;\beta_{k+1}), \qquad (4)$$

находим, используя имеющийся в наличии метод построения примитивного элемента для составных алгебраических расширений порядка 2, примитивный элемент для расширения $\mathcal{P}(\theta;\beta_{k+1})$, т. е. такой элемент $\theta \in F$, что

$$\mathcal{P}(\theta;\beta_{k+1}) = \mathcal{P}(\theta). \qquad (5)$$

Из равенств (4) и (5) тогда получим, что

$$\mathcal{P}(\beta_1;\beta_2;\ldots;\beta_k;\beta_{k+1}) = \mathcal{P}(\theta).$$

Следуя доказательству теоремы о примитивном элементе, укажем теперь способ построения примитивного элемента θ для составного алгебраического расширения $\boldsymbol{P}\ \alpha;\beta$ поля $\boldsymbol{P}$ порядка 2.

Пусть α и β - алгебраические над $\boldsymbol{P}$ элементы степеней m и n, соответственно и $\alpha=\alpha_1;\alpha_2;...;\alpha_m$ - корни минимального многочлена $f_1\ x$ для элемента α, а $\beta=\beta_1;\beta_2;...;\beta_n$ - корни минимального многочлена $f_2\ x$ для элемента β. Тогда примитивный элемент θ для составного алгебраического расширения ищется в виде $\theta=\alpha+c\beta$, где c - любой элемент поля $\boldsymbol{P}$, отличный от всех корней линейных уравнений

$$\alpha_i+\beta_k x=\alpha_1+\beta_1 x,\ i=1;2;...;m;\ j=2;3;...;n. \qquad (6)$$

Так как число уравнений вида (6) равно $m\cdot\ n-1$, т. е. конечно, а поле $\boldsymbol{P}$, как поле нулевой характеристики, бесконечно, то элемент c поля $\boldsymbol{P}$ с указанными свойствами всегда найдется.

5. Как отмечалось ранее, в качестве поля $\boldsymbol{P}$ будем рассматривать поле $\boldsymbol{Q}$ - рациональных чисел, а в качестве поля $\boldsymbol{F}$ - поле $\boldsymbol{C}$ - комплексных чисел. Так как поле $\boldsymbol{C}$ - алгебраически замкнуто, то все дальнейшие построения, связанные с корнями многочленов из кольца $\boldsymbol{Q}\ x$ будут осуществляться в пределах поля $\boldsymbol{C}$.

Числа $\alpha=\sqrt{2}$; $\beta=\sqrt{3}$ и $\gamma=i$ являются алгебраическими над полем $\boldsymbol{Q}$. Поле $\boldsymbol{Q}\ \sqrt{2};\sqrt{3};i$, как составное алгебраическое расширение поля $\boldsymbol{Q}$ порядка 3 может быть получено в результате трех последовательных простых алгебраических расширений, образующих следующую возрастающую цепочку подполей поля $\boldsymbol{C}$:

$$\boldsymbol{Q}\prec\boldsymbol{Q}\ \sqrt{2}\ \prec\boldsymbol{Q}\ \sqrt{2};\sqrt{3}\ \prec\boldsymbol{Q}\ \sqrt{2};\sqrt{3};i\ .$$

Каждое последующее поле этой цепочки, как векторное пространство над предшествующим, имеет размерность 2. В приведенной ниже таблице (таблица 1) указаны размерности и базисы этих подпространств, а также минимальные многочлены присоединяемых элементов и их корни.

Таблица 1 – Описание векторных пространств

Пространство	Размерность	Базис	Характеристический многочлен	Корни
$Q(\sqrt{2})$ над Q	2	$1;\sqrt{2}$	$f_1(x)=x^2-2$	$\alpha_1=\sqrt{2};$ $\alpha_2=-\sqrt{2}$
$Q(\sqrt{2};\sqrt{3})$ над $Q(\sqrt{2})$	2	$1;\sqrt{3}$	$f_2(x)=x^2-3$	$\beta_1=\sqrt{3};$ $\beta_2=-\sqrt{3}$
$Q(\sqrt{2};\sqrt{3};i)$ над $Q(\sqrt{2};\sqrt{3})$	2	$1;i$	$f_3(x)=x^2+1$	$\gamma_1=i;$ $\gamma_2=-i$

$$Q(\sqrt{2}) \subset Q(\sqrt{2};\sqrt{3}) \subset Q(\sqrt{2};\sqrt{3};i)$$

6. В соответствии с вышеприведенным порядком нахождения примитивного элемента θ для составного алгебраического расширения порядка 2, выпишем для расширения $Q(\sqrt{2};\sqrt{3})$ все уравнения вида (6). Так как в рассматриваемом случае, $m=n=2$, то получим два таких уравнения:

1) $\sqrt{2}+(-\sqrt{3})x=\sqrt{2}+\sqrt{3}x$;

2) $-\sqrt{2}+(-\sqrt{3})x=\sqrt{2}+\sqrt{3}x$.

Так как корнями этих уравнений являются, соответственно, числа 0 и $-\frac{2\sqrt{2}}{\sqrt{3}}$, то в качестве c можно взять любое рациональное число отличное от нуля, в частности, число 1. Таким образом, число $\theta_1=\sqrt{2}+\sqrt{3}$ является примитивным элементом и, следовательно,

$$Q(\sqrt{2};\sqrt{3})=Q(\sqrt{2}+\sqrt{3}). \qquad (7)$$

Так как $\left[Q(\sqrt{2};\sqrt{3}):Q(\sqrt{2})\right]=\left[Q(\sqrt{2}):Q\right]=2$, то основываясь на теореме 2, получаем, что $\left[Q(\sqrt{2}):Q\right]=2\cdot 2=4$ и элементы

$1;\sqrt{2};\sqrt{3};\sqrt{6}$ составляют базис поля $Q(\sqrt{2};\sqrt{3})$, как векторного пространства над полем Q. Отметим, что согласно теореме 1, элементы $1;\theta_1;\theta_1^2;\theta_1^3$, т. е. элементы 1; $\sqrt{2}+\sqrt{3}$; $5+2\sqrt{6}$; $11\sqrt{2}+9\sqrt{3}$, образуют другой базис поля $Q(\sqrt{2};\sqrt{3})$ над Q. Для нахождения минимального многочлена $g(x)$ из кольца $Q[x]$ для элемента $\theta_1=\sqrt{2}+\sqrt{3}$ можно поступить следующим образом. Полагая $x=\sqrt{2}+\sqrt{3}$, осуществим ряд следующих очевидных преобразований:

$$x^2=(\sqrt{2}+\sqrt{3})^2; \qquad x^2-5=2\sqrt{6};$$

$$(x^2-5)^2=(2\sqrt{6})^2; \qquad x^4-10x^2+1=0.$$

Отсюда получаем, что число $\theta_1=\sqrt{2}+\sqrt{3}$ является корнем многочлена $g(x)=x^4-10x^2+1$. Так как степень многочлена $g(x)$ равна 4, т. е. совпадают с размерностью поля $Q(\sqrt{2};\sqrt{3})$ над Q, и этот многочлен является нормированным, то он действительно будет минимальным многочленом элемента $\theta_1=\sqrt{2}+\sqrt{3}$. Находя корни этого многочлена (т. е. решая биквадратное уравнение $x^4-10x^2+1=0$), получим:

$$\theta=\theta_1=\sqrt{2}+\sqrt{3}; \qquad \theta_2=\sqrt{2}-\sqrt{3};$$
$$\theta_3=-\sqrt{2}+\sqrt{3}; \qquad \theta_4=-\sqrt{2}-\sqrt{3}.$$

7. Согласно описанию индукционного шага в построении примитивного элемента для составного алгебраического расширения порядка $t>2$, примитивный элемент θ для расширения $Q(\sqrt{2};\sqrt{3};i)$ будем искать, как примитивный элемент для расширения $Q(\theta_1;i)=Q(\sqrt{2};\sqrt{3};i)$ (смотри равенство 7), т. е. в виде $\theta=\theta_1+c_1 i$, где c_1 - любой элемент поля Q, отличный от корней всех уравнений вида (6). В рассматриваемом случае, т. е. при $m=4$; $n=2$, число

таких уравнений будет равно 4. Выписывая совокупность этих уравнений применительно к $\alpha=\sqrt{2}+\sqrt{3}$ и $\beta=i$, получим:

1. $(\sqrt{2}+\sqrt{3})+(-i)x=(\sqrt{2}+\sqrt{3})+ix$;
2. $(\sqrt{2}-\sqrt{3})+(-i)x=(\sqrt{2}+\sqrt{3})+ix$;
3. $(-\sqrt{2}+\sqrt{3})+(-i)x=(\sqrt{2}+\sqrt{3})+ix$;
4. $(-\sqrt{2}-\sqrt{3})+(-i)x=(\sqrt{2}+\sqrt{3})+ix$.

Корнями этих уравнений является, соответственно, числа $0;\sqrt{3}i;\sqrt{2}i;(\sqrt{2}+\sqrt{3})i$. Таким образом, в качестве c_1 также можно взять число $1\in Q$ и, следовательно, в качестве примитивного элемента θ -число $\theta=\sqrt{2}+\sqrt{3}+i$.

Аналогично процедуре нахождения минимального многочлена $q(x)$ для алгебраического элемента $\theta_1=\sqrt{2}+\sqrt{3}$, находим минимальный многочлен $h(x)$ для элемента $\theta=\sqrt{2}+\sqrt{3}+i$. Заметим, что т. к.

$$\left[Q(\sqrt{2}+\sqrt{3}+i):Q\right]=\left[Q(\sqrt{2}+\sqrt{3};i):Q\right]=$$
$$=\left[Q(\sqrt{2}+\sqrt{3};i):Q(\sqrt{2}+\sqrt{3})\right]\cdot\left[Q(\sqrt{2}+\sqrt{3}):Q\right]=2\cdot4=8,$$

то степень многочлена $h(x)$ должна быть ровна 8.

Полагая $x=\sqrt{2}+\sqrt{3}+i$, будем иметь:

$$(x-\sqrt{2})^2=(\sqrt{3}+i)^2;$$
$$x^2-2\sqrt{2}x+2=3+2\sqrt{3}i-1;$$
$$(x^2-2\sqrt{2}x)^2=(2\sqrt{3}i)^2;$$
$$x^4-4\sqrt{2}x^3+8x^2=-12;$$
$$(x^4+8x^2+12)^2=(4\sqrt{2}x^3)^2;$$
$$x^8+16x^6+24x^4+64x^4+192x^2+144=32x^6;$$
$$x^8-16x^6+88x^4+192x^2+144=0$$

Отсюда получаем, что многочлен

$$h(x)=x^8-16x^6+88x^4+192x^2+144$$

является минимальным для элемента $\theta=\sqrt{2}+\sqrt{3}+i$.

Сводя уравнения $h(x)=0$ к уравнению

$$y^4-16y^3+88y^2+192y+144=0$$

и решая это уравнение, известными методами вышей алгебры, получим его корни:

$$\begin{aligned} \theta = \theta_1 &= \sqrt{2}+\sqrt{3}+i; & \theta_5 &= -\sqrt{2}-\sqrt{3}+i; \\ \theta_2 &= \sqrt{2}+\sqrt{3}-i; & \theta_6 &= -\sqrt{2}+\sqrt{3}-i; \\ \theta_3 &= -\sqrt{2}+\sqrt{3}+i; & \theta_7 &= \sqrt{2}-\sqrt{3}-i; \\ \theta_4 &= \sqrt{2}-\sqrt{3}+i; & \theta_8 &= -\sqrt{2}-\sqrt{3}-i \end{aligned} \qquad (8)$$

8. Т. к. элементы $1;\sqrt{2};\sqrt{3};\sqrt{6}$ образует базис пространства $\boldsymbol{Q}(\sqrt{2};\sqrt{3})$ над полем $\boldsymbol{Q}$ а элементы $1;\ i$ - образуют базис пространства $\boldsymbol{Q}(\sqrt{2};\sqrt{3};i)$ (под полем $\boldsymbol{Q}(\sqrt{2};\sqrt{3})$), то, согласно теореме 2, элементы:

$$1;\ \sqrt{2};\ \sqrt{3};\ \sqrt{6};\ i;\ i\sqrt{2};\ i\sqrt{3};\ i\sqrt{6} \qquad (9)$$

составляют базис пространства $\boldsymbol{Q}(\sqrt{2};\sqrt{3};i)=\boldsymbol{Q}(\sqrt{2}+\sqrt{3}+i)$ над полем $\boldsymbol{Q}$. С другой стороны, по теореме 1, элементы $1;\ \theta;\ \theta^2;\ \theta^3;\ \theta^4;\ \theta^5;\ \theta^6;\theta^7$ т.е элементы:

$$\begin{aligned} &1;\quad \sqrt{2}+\sqrt{3}+i;\quad 4+2\sqrt{6}+2\sqrt{2}i+2\sqrt{3}i;\quad 8\sqrt{2}+6\sqrt{3}+14i+6\sqrt{6}i; \\ &20+8\sqrt{6}+40\sqrt{2}i+32\sqrt{3}i;\quad 4\sqrt{2}+4\sqrt{3}+196i+80\sqrt{6}i;\quad -176-72\sqrt{6}+ \\ &+440\sqrt{2}i+360\sqrt{3}i;\ -832\sqrt{2}\ -680\sqrt{3}+1784i+728\sqrt{6}i \end{aligned} \qquad (10)$$

составляют второй базис поля $\boldsymbol{Q}(\sqrt{2};\sqrt{3};i)$ над полем $\boldsymbol{Q}$.

Находя матрицу T перехода от базиса (9) к базису (10)получим:

$$T=\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 4 & 0 & 0 & 2 & 0 & 2 & 2 & 0 \\ 0 & 8 & 6 & 0 & 14 & 0 & 0 & 6 \\ 20 & 0 & 0 & 8 & 0 & 40 & 32 & 0 \\ 0 & 4 & 4 & 0 & 196 & 0 & 0 & 80 \\ -176 & 0 & 0 & -72 & 0 & 440 & 360 & 0 \\ 0 & -832 & -680 & 0 & 1784 & 0 & 0 & 728 \end{pmatrix}$$

Матрицу перехода от базиса (10) к базису (9) найдем, как матрицу, обратную по отношению к матрице T. Вычисляя матрицу T^{-1}, получим:

$$T^{-1}=\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{13}{12} & 0 & \frac{14}{9} & 0 & -\frac{35}{144} & 0 & \frac{1}{72} \\ 0 & -\frac{21}{16} & 0 & -\frac{181}{96} & 0 & \frac{59}{192} & 0 & -\frac{7}{384} \\ -\frac{19}{8} & 0 & \frac{5}{48} & 0 & \frac{5}{96} & 0 & -\frac{1}{192} & 0 \\ 0 & \frac{59}{48} & 0 & \frac{95}{288} & 0 & -\frac{37}{576} & 0 & \frac{5}{1152} \\ -\frac{13}{8} & 0 & -\frac{27}{16} & 0 & \frac{9}{32} & 0 & -\frac{1}{64} & 0 \\ 2 & 0 & \frac{25}{12} & 0 & -\frac{1}{3} & 0 & \frac{1}{48} & 0 \\ 0 & -3 & 0 & -\frac{19}{24} & 0 & \frac{1}{6} & 0 & -\frac{1}{96} \end{pmatrix}.$$

Т.к. строки матрицы T^{-1} являются координатными строками элементов базиса (9) в базисе (10), то

$$\begin{aligned} \sqrt{2} &= \frac{13}{12}\theta_1+\frac{14}{9}\theta_1^3-\frac{35}{144}\theta_1^5+\frac{1}{72}\theta_1^7; \\ \sqrt{3} &= -\frac{21}{16}\theta_1-\frac{181}{96}\theta_1^3+\frac{59}{192}\theta_1^5-\frac{7}{384}\theta_1^7; \\ \sqrt{6} &= -\frac{19}{8}+\frac{5}{48}\theta_1^2+\frac{5}{96}\theta_1^4-\frac{1}{192}\theta_1^6; \\ i &= \frac{59}{48}\theta_1+\frac{95}{288}\theta_1^3-\frac{37}{576}\theta_1^5+\frac{5}{1152}\theta_1^7; \\ i\sqrt{2} &= -\frac{13}{8}-\frac{27}{16}\theta_1^2+\frac{9}{32}\theta_1^4-\frac{1}{64}\theta_1^6; \\ i\sqrt{3} &= 2+\frac{25}{12}\theta_1^2-\frac{1}{3}\theta_1^4+\frac{1}{48}\theta_1^6; \\ i\sqrt{6} &= -3\theta_1-\frac{19}{24}\theta_1^3+\frac{1}{6}\theta_1^5-\frac{1}{96}\theta_1^7. \end{aligned} \qquad (11)$$

9. Имея разложение чисел $\sqrt{2};\sqrt{3};i$ по элементам базиса (10), получаем возможность выразить корни θ_i $i=2;3;...;8$ уравнения

$$x^8-16x^6+88x^4+192x^2+144=0$$

через θ_1. К примеру,

$$\theta_2 = \sqrt{2}+\sqrt{3}-i = \left(\frac{13}{12}\theta_1 + \frac{14}{9}\theta_1^3 - \frac{35}{144}\theta_1^5 + \frac{1}{72}\theta_1^7\right) +$$

$$+\left(-\frac{21}{16}\theta_1 - \frac{181}{96}\theta_1^3 + \frac{59}{192}\theta_1^5 - \frac{7}{384}\theta_1^7\right) - \left(\frac{59}{48}\theta_1 + \frac{95}{288}\theta_1^3 - \frac{37}{576}\theta_1^5 + \frac{5}{1152}\theta_1^7\right) =$$

$$= -\frac{35}{24}\theta_1 - \frac{95}{144}\theta_1^3 + \frac{37}{288}\theta_1^5 - \frac{5}{192}\theta_1^7 .$$

Аналогичным образом получаем выражение других корней через θ_1. В результате будем иметь:

$$\begin{aligned}
\theta_2 &= -\frac{35}{24}\theta_1 - \frac{95}{144}\theta_1^3 + \frac{37}{288}\theta_1^5 - \frac{5}{576}\theta_1^7;\\
\theta_3 &= -\frac{7}{6}\theta_1 - \frac{28}{9}\theta_1^3 + \frac{35}{72}\theta_1^5 - \frac{1}{36}\theta_1^7;\\
\theta_4 &= \frac{87}{24}\theta_1 + \frac{543}{144}\theta_1^3 - \frac{59}{96}\theta_1^5 + \frac{7}{192}\theta_1^7;\\
\theta_5 &= \frac{35}{24}\theta_1 + \frac{95}{144}\theta_1^3 - \frac{37}{288}\theta_1^5 + \frac{5}{576}\theta_1^7;\\
\theta_6 &= -\frac{87}{24}\theta_1 - \frac{28}{9}\theta_1^3 + \frac{59}{96}\theta_1^5 - \frac{7}{192}\theta_1^7;\\
\theta_7 &= \frac{7}{6}\theta_1 + \frac{28}{9}\theta_1^3 - \frac{35}{72}\theta_1^5 + \frac{1}{36}\theta_1^7;\\
\theta_8 &= -\theta_1
\end{aligned} \qquad (12)$$

Заметим, что к этим же самым результатам можно прийти, рассматривая поле $\boldsymbol{Q}(\theta)$ как векторное пространство под полем $\boldsymbol{Q}$ и используя связь между координатными строками одного и того же вектора этого пространства в разных базисах.

Так как координатными строками корней $\theta_2;\theta_3;\theta_4;\theta_5;\theta_6;\theta_7$ и θ_8, как векторов пространства $\boldsymbol{Q}(\theta)$, является строки:

$a\ \theta_2 = 0;1;1;0;-1;0;0;0$;
$a\ \theta_3 = 0;-1;1;0;1;0;0;0$;
$a\ \theta_4 = 0;1;-1;0;1;0;0;0$;
$a\ \theta_5 = 0;-1;-1;0;1;0;0;0$;
$a\ \theta_6 = 0;-1;1;0;-1;0;0;0$;
$a\ \theta_7 = 0;1;-1;0;-1;0;0;0$;
$a\ \theta_8 = 0;-1;-1;0;-1;0;0;0$,

то:

$$a'\ \theta_2 = 0;1;1;0;-1;0;0;0\ \cdot T^{-1} = \left(0;-\frac{35}{24};0;-\frac{95}{144};0\frac{37}{288};0;\frac{5}{192}\right);$$

$$a'\ \theta_3 = 0;-1;1;0;1;0;0;0\ \cdot T^{-1} = \left(0;-\frac{7}{6};0;-\frac{28}{9};0;\frac{35}{72};0;-\frac{1}{36}\right);$$

$$a'\ \theta_4 = 0;1;-1;0;1;0;0;0\ \cdot T^{-1} = \left(0;\frac{87}{24};0;\frac{543}{144};0;-\frac{59}{96};0;\frac{7}{192}\right);$$

$$a'\ \theta_5 = 0;-1;-1;0;1;0;0;0\ \cdot T^{-1} = \left(0;\frac{35}{24};0;\frac{95}{144};0;-\frac{37}{288};0;\frac{5}{576}\right);$$

$$a'\ \theta_6 = 0;-1;1;0;-1;0;0;0\ \cdot T^{-1} = \left(0;-\frac{87}{24};0;-\frac{28}{9};0;\frac{59}{96};0;-\frac{7}{192}\right);$$

$$a'\ \theta_7 = 0;1;-1;0;-1;0;0;0\ \cdot T^{-1} = \left(0;\frac{7}{6};0;\frac{28}{9};0;-\frac{35}{72};0;\frac{1}{36}\right);$$

$$a'\ \theta_8 = 0;-1;-1;0;-1;0;0;0\ \cdot T^{-1} = 0;-1;0;0;0;0;0;0\ .$$

10. Т. к. размерность поля $\boldsymbol{Q}\ \theta$ над $\boldsymbol{Q}$ равна 8, то группа Галуа $\boldsymbol{G}\left(\boldsymbol{Q}\ \theta \Big/ \boldsymbol{Q}\right)$ является конечной группой 8-го порядка. При автоморфизмах поля $\boldsymbol{Q}\ \theta$ над $\boldsymbol{Q}$ примитивный элемент $\theta = \theta_1$ переходит в сопряженные с ним элементы, т. е. в корни $\theta_1;\theta_2;...;\theta_8$ и каждый из этих автоморфизмов полностью определяется образом элемента θ. Обозначим через Φ_i автоморфизм, при котором θ переходит в θ_i, т. е.

$$\Phi_i : \boldsymbol{Q}\ \theta \Big/ \boldsymbol{Q} \to \boldsymbol{Q}\ Q \Big/ \boldsymbol{Q} \text{ и } \Phi_i\ \theta = \theta_i \quad i = 1;2;...;8\ .$$

Таким образом, подстановка корней, соответствующая автоморфизму Φ_i, будет иметь вид:

$$\begin{pmatrix} \theta_1 & \theta_2 & \theta_3 & ... & \theta_8 \\ \theta_i & \Phi_i\ \theta_2 & \Phi_i\ \theta_3 & ... & \Phi_i\ \theta_8 \end{pmatrix},\ i = 2;3;...;8 \qquad (13)$$

а соответствующая подстановка π_i симметрической группы S_8 - вид:

$$\begin{pmatrix} 1 & 2 & 3 & ... & i & ... & 8 \\ i & \alpha_2 & \alpha_3 & ... & \alpha_i & ... & \alpha_8 \end{pmatrix},$$

где α_i - номер корня $\Phi_i\ \theta_j$, $j = 2;3;...;8$; $i = 2;3;...;8$.

Заметим, что при $i=1$ получаем тождественный автоморфизм Φ_1, которому соответствует тождественная подстановка корней, т. е. π_1 - нейтральный элемент группы S_8.

Согласно виду (12) представления корней, для нахождения подстановки $\pi_i \in S_8$, соответствующей автоморфизму Φ_i, нужно найти образы $\Phi_i\ \theta_2$; $\Phi_i\ \theta_3$;...;$\Phi_i\ \theta_8$, $i=2;3;...;8$.

Сделать это можно:

а) применяя равенства (11);

б) используя систему равенств (12);

в) основываясь на теореме о продолжении изоморфизмов.

Реализация возможностей а), б) связана с непосредственным выполнением вычислительных процедур. Несмотря на их однообразие и громоздкость, эти вычисления напрямую приводят к требуемым результатам, без привлечения каких-то дополнительных соображений.

Приведем, для примера, вычисления, необходимые для нахождения подстановки π_7, следуя возможности а).

а.1) Вычисляем: $\Phi_7\ \sqrt{2}$; $\Phi_7\ \sqrt{3}$; $\Phi_7\ i$.

$$\Phi_7\ \sqrt{2} = \Phi_7\left(\frac{13}{12}\theta_1+\frac{14}{9}\theta_1^3-\frac{35}{144}\theta_1^5+\frac{1}{72}\theta_1^7\right)=\frac{13}{12}\Phi_7\ \theta_1+\frac{14}{9}\Phi_7\ \theta_1^3-$$

$$-\frac{35}{144}\Phi_7\ \theta_1^5+\frac{1}{72}\Phi_7\ \theta_1^7=\frac{13}{12}\theta_7+\frac{14}{9}\theta_7^3-\frac{35}{144}\theta_7^5+\frac{1}{72}\theta_7^7=\frac{13}{12}\sqrt{2}-\sqrt{3}-i+$$

$$+\frac{14}{9}\left(\sqrt{2}-\sqrt{3}-i\right)^3-\frac{35}{144}\left(\sqrt{2}-\sqrt{3}-i\right)^5+\frac{1}{72}\left(\sqrt{2}-\sqrt{3}-i\right)^7=\frac{13}{12}\sqrt{2}-\frac{13}{12}\sqrt{3}-$$

$$-\frac{13}{12}i+\frac{14}{9}\left(8\sqrt{2}-6\sqrt{3}+6\sqrt{6}i-14i\right)-\frac{35}{144}\left(4\sqrt{2}-4\sqrt{3}+80\sqrt{6}i-196i\right)+$$

$$+\frac{1}{72}\left(-832\sqrt{2}+680\sqrt{3}+728\sqrt{6}i-1784i\right)=\frac{39+448-35-416}{36}\sqrt{2}+$$

$$+\frac{-39-336+35+340}{36}\sqrt{3}+\frac{84-175+91}{9}\sqrt{6}i+\frac{-39-784+1715-892}{36}i=\sqrt{2}$$

$$\Phi_7\ \sqrt{3} = \Phi_7\left(-\frac{21}{16}\theta_1-\frac{181}{96}\theta_1^3+\frac{59}{192}\theta_1^5-\frac{7}{384}\theta_1^7\right)=-\frac{21}{16}\Phi_7\ \theta_1-$$

$$-\frac{181}{96}\Phi_7\ \theta_1^3+\frac{59}{192}\Phi_7\ \theta_1^5-\frac{7}{384}\Phi_7\ \theta_1^7=-\frac{21}{16}\theta_7-\frac{181}{96}\theta_7^3+\frac{59}{192}\theta_7^5-\frac{7}{384}\theta_7^7=$$

$$= -\frac{21}{16}\left(\sqrt{2}-\sqrt{3}-i\right) - \frac{181}{96}\left(\sqrt{2}-\sqrt{3}-i\right)^3 + \frac{59}{192}\left(\sqrt{2}-\sqrt{3}-i\right)^5 -$$

$$-\frac{7}{384}\left(\sqrt{2}-\sqrt{3}-i\right)^7 = -\frac{21}{16}\sqrt{2}+\frac{21}{16}\sqrt{3}+\frac{21}{16}i-\frac{181}{96}\left(8\sqrt{2}-6\sqrt{3}+6\sqrt{6}i-14i\right) +$$

$$+\frac{59}{192}\left(4\sqrt{2}-4\sqrt{3}+80\sqrt{6}i-196i\right) - \frac{7}{384}\left(-832\sqrt{2}+680\sqrt{3}+728\sqrt{6}i-1784i\right) =$$

$$= \frac{-63-724+59+728}{48}\sqrt{2} + \frac{63+543-59-595}{48}\sqrt{3} + \frac{-543+1180-637}{48}\sqrt{6}i +$$

$$+\frac{63+1267-2891+1561}{48}i = -\sqrt{3}$$

$$\Phi_7\left(i\right) = \Phi_7\left(\frac{59}{48}\theta_1 + \frac{95}{288}\theta_1^3 - \frac{37}{576}\theta_1^5 + \frac{5}{1152}\theta_1^7\right) = \frac{59}{48}\Phi_7\left(\theta_1\right) + \frac{95}{288}\Phi_7\left(\theta_1^3\right) -$$

$$-\frac{37}{576}\Phi_7\left(\theta_1^5\right) + \frac{5}{1182}\Phi_7\left(\theta_1^7\right) = \frac{59}{48}\theta_7 + \frac{95}{288}\theta_7^3 - \frac{37}{576}\theta_7^5 + \frac{5}{1152}\theta_7^7 =$$

$$= \frac{59}{48}\left(\sqrt{2}-\sqrt{3}-i\right) + \frac{95}{288}\left(\sqrt{2}-\sqrt{3}-i\right)^3 - \frac{37}{576}\left(\sqrt{2}-\sqrt{3}-i\right)^5 +$$

$$+\frac{5}{1152}\left(\sqrt{2}-\sqrt{3}-i\right)^7 = \frac{59}{48}\sqrt{2}-\frac{59}{48}\sqrt{3}-\frac{59}{48}i+\frac{95}{288}\left(8\sqrt{2}-6\sqrt{3}+6\sqrt{6}i-14i\right) -$$

$$-\frac{37}{576}\left(4\sqrt{2}-4\sqrt{3}+80\sqrt{6}i-196i\right) + \frac{5}{1152}\left(-832\sqrt{2}+680\sqrt{3}+728\sqrt{6}i-1784i\right) =$$

$$= \frac{177+380-37-520}{144}\sqrt{2} + \frac{-177-285+37+425}{144}\sqrt{3} + \frac{285-740+455}{144}\sqrt{6}i +$$

$$+\frac{-177-665+1813-1115}{144}i = -i$$

а.2) Далее находим $\Phi_7\left(\theta_2\right)$; $\Phi_7\left(\theta_3\right)$;...;$\Phi_7\left(\theta_8\right)$.

$$\Phi_7\left(\theta_2\right) = \Phi_7\left(\sqrt{2}+\sqrt{3}-i\right) = \Phi_7\left(\sqrt{2}\right) + \Phi_7\left(\sqrt{3}\right) - \Phi_7\left(i\right) = \sqrt{2}-\sqrt{3}+i = \theta_4;$$

$$\Phi_7\left(\theta_3\right) = \Phi_7\left(-\sqrt{2}+\sqrt{3}+i\right) = -\Phi_7\left(\sqrt{2}\right) + \Phi_7\left(\sqrt{3}\right) + \Phi_7\left(i\right) = -\sqrt{2}-\sqrt{3}-i = \theta_8;$$

$$\Phi_7\left(\theta_4\right) = \Phi_7\left(\sqrt{2}-\sqrt{3}+i\right) = \Phi_7\left(\sqrt{2}\right) - \Phi_7\left(\sqrt{3}\right) + \Phi_7\left(i\right) = \sqrt{2}+\sqrt{3}-i = \theta_2;$$

$$\Phi_7\left(\theta_5\right) = \Phi_7\left(-\sqrt{2}-\sqrt{3}+i\right) = -\Phi_7\left(\sqrt{2}\right) - \Phi_7\left(\sqrt{3}\right) + \Phi_7\left(i\right) = -\sqrt{2}+\sqrt{3}-i = \theta_6;$$

$$\Phi_7\left(\theta_6\right) = \Phi_7\left(-\sqrt{2}+\sqrt{3}-i\right) = -\Phi_7\left(\sqrt{2}\right) + \Phi_7\left(\sqrt{3}\right) - \Phi_7\left(i\right) = -\sqrt{2}-\sqrt{3}+i = \theta_5;$$

$$\Phi_7(\theta_7)=\Phi_7\left(\sqrt{2}-\sqrt{3}-i\right)=\Phi_7\left(\sqrt{2}\right)-\Phi_7\left(\sqrt{3}\right)-\Phi_7(i)=\sqrt{2}+\sqrt{3}+i=\theta_1;$$

$$\Phi_7(\theta_8)=\Phi_7\left(-\sqrt{2}-\sqrt{3}-i\right)=-\Phi_7\left(\sqrt{2}\right)-\Phi_7\left(\sqrt{3}\right)-\Phi_7(i)=-\sqrt{2}+\sqrt{3}+i=\theta_3.$$

Следовательно, соответствующая автоморфизму Φ_7 подстановка корней будет такой: $\begin{pmatrix}\theta_1 & \theta_2 & \theta_3 & \theta_4 & \theta_5 & \theta_6 & \theta_7 & \theta_8\\ \theta_7 & \theta_4 & \theta_8 & \theta_2 & \theta_6 & \theta_5 & \theta_1 & \theta_3\end{pmatrix}$, т. е.

$$\pi_7=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 7 & 4 & 8 & 2 & 6 & 5 & 1 & 3\end{pmatrix}.$$

б) Вычисление подстановки π_4 (к примеру), осуществленное на основе системы равенств (12), будет выглядеть следующим образом:

$$\Phi_4(\theta_2)=\Phi_4\left(-\frac{35}{24}\theta_1-\frac{95}{144}\theta_1^3+\frac{37}{288}\theta_1^5-\frac{5}{576}\theta_1^7\right)=-\frac{35}{24}\Phi_4(\theta_1)-$$

$$-\frac{95}{144}\Phi_4\left(\theta_1^3\right)+\frac{37}{288}\Phi_4\left(\theta_1^5\right)-\frac{5}{192}\Phi_4\left(\theta_1^7\right)=-\frac{35}{24}\left(\sqrt{2}-\sqrt{3}+i\right)-$$

$$-\frac{95}{144}\left(\sqrt{2}-\sqrt{3}+i\right)^3+\frac{37}{288}\left(\sqrt{2}-\sqrt{3}+i\right)^5-\frac{5}{576}\left(\sqrt{2}-\sqrt{3}+i\right)^7=-\frac{35}{24}\sqrt{2}+$$

$$+\frac{35}{24}\sqrt{3}-\frac{35}{24}i-\frac{95}{144}\left(8\sqrt{2}-6\sqrt{3}-6\sqrt{6}i+14i\right)+\frac{37}{288}\left(4\sqrt{2}-4\sqrt{3}-80\sqrt{6}i+196i\right)-$$

$$-\frac{5}{576}\left(-832\sqrt{2}+680\sqrt{3}-728\sqrt{6}i+1784i\right)=\left(-\frac{35}{24}-\frac{95}{18}+\frac{37}{72}+\frac{65}{9}\right)\sqrt{2}+$$

$$+\left(\frac{35}{24}+\frac{95}{24}-\frac{37}{72}-\frac{425}{72}\right)\sqrt{3}+\left(\frac{95}{24}-\frac{185}{18}+\frac{455}{72}\right)\sqrt{6}i+$$

$$+\left(-\frac{35}{24}-\frac{665}{72}+\frac{1813}{72}-\frac{1115}{72}\right)i=\frac{-105-380+37+520}{72}\sqrt{2}+$$

$$+\frac{105+285-37-425}{72}\sqrt{3}+\frac{285-740+455}{72}\sqrt{6}i+\frac{-105-665+1813-1115}{72}i=$$

$$\sqrt{2}-\sqrt{3}-i=\theta_7.$$

Аналогичным образом находим:

$$\Phi_4(\theta_3)=\theta_5;\Phi_4(\theta_4)=\theta_1;\Phi_4(\theta_5)=\theta_3;\Phi_4(\theta_6)=\theta_8;\Phi_4(\theta_7)=\theta_2;\Phi_4(\theta_8)=\theta_6,$$

т. е. соответствующая автоморфизму Φ_4 подстановка корней будет такой: $\begin{pmatrix}\theta_1 & \theta_2 & \theta_3 & \theta_4 & \theta_5 & \theta_6 & \theta_7 & \theta_8\\ \theta_4 & \theta_7 & \theta_5 & \theta_1 & \theta_3 & \theta_8 & \theta_2 & \theta_6\end{pmatrix}$ и, следовательно

$$\pi_4=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 4 & 7 & 5 & 1 & 3 & 8 & 2 & 6\end{pmatrix}.$$

СПИСОК ЛИТЕРАТУРЫ

1. **Ван дер Варден, Б. Л.** Алгебра. - 2-е издание. - М. : Наука, 1979. – 623 с.

2. **Каргаполов, М. И., Мерзляков, Ю. И.** Основы теории групп. – 3-е издание. – М. : Наука, 1982. – 288 с.

Павлодарский государственный университет
имени С. Торайгырова, Павлодар.
Материал поступил в редакцию 26.03.13.

Б. Н. Дроботун, О. И. Панасенко

Галуа топтары және рационал сандар өрісінің ақырлы кеңей тілулерінің Галуа үйлесімділігі (I)

С. Торайғыров атындағы Павлодар
мемлекеттік университеті, Павлодар қ.
Материал 26.03.13 редакцияға түсті.

B. N. Drobotun, O. I. Panasenko

Galoi's groups and adequacies of final extension of the field of rational numbers (I)

Pavlodar State University named after S. Toraigyrov, Pavlodar.
Material received on 26.03.13.

Жогары оқу орындарында Галуа теориясының негіздерін меңгеруде әдінамалық тәсілдерді жасауға арналған берілген жұмыста алмастыру топтарының ішкітаптары негізінде рационал сандар өрістерінің (деңгей 2) құрамды алгебралық

кеңей тілулері Галуа топтарының көрінісе ретінде технологиялық сипаттамасы беріледі.

In this work devoting to the working out of the methodological ways of the studying foundation of Galoi's theory in the higher establishments the description of the technologies of the presenting of the Galoi's group of the composite algebraic extension(degree -2) of the field of rational numbers by means of the subgroups of the group of substitutions is given.

УДК 511.238

Б. Н. Дроботун, О. И. Панасенко

ГРУППЫ ГАЛУА И СООТВЕТСТВИЯ ГАЛУА КОНЕЧНЫХ РАСШИРЕНИЙ ПОЛЯ РАЦИОНАЛЬНЫХ ЧИСЕЛ (II)

В данной работе, посвященной разработке методологических подходов к изучению основ теории Галуа в высших учебных заведениях, предлагается описание технологий выявления структур подгрупп группы Галуа и подполей составных алгебраических расширений (степени 2) поля рациональных чисел и построения соответствия Галуа между этими структурами.

11. Данная статья, является непосредственным продолжением статьи [1] и представляет собой вторую часть работы, посвященной разработке технологических подходов к изучению основ теории Галуа в высших учебных заведениях. В ней предлагаются технологические подходы к выявлению структуры подгрупп группы $G\left(\boldsymbol{Q}(\sqrt{2};\sqrt{3};i)\middle/\boldsymbol{Q}\right)$, полученной в [1], и структуры подполей поля $\boldsymbol{Q}\left(\sqrt{2};\sqrt{3};i\right)$, а также установлению соответствия Галуа между этими структурами.

Как уже отмечалось в [1], предлагаемые технологии, описание которых дается применительно к расширению $\boldsymbol{Q}\left(\sqrt{2};\sqrt{3};i\right)$ поля

рациональных чисел Q, аккумулирует в себе возможности их обобщения на случай расширения $Q(\alpha_1;\alpha_2;...;\alpha_t)$, где $\alpha_1;\alpha_2;...;\alpha_t (t>3)$ любая конечная совокупность алгебраических на полем Q элементов степени 2.

С целью обеспечения удобства ссылок, нумерации разделов, таблиц и формул статьи [1], в данной статье находят естественное продолжение.

12. В разделе 10 статьи [1] были реализованы возможности представления автоморфизмов группы $G\left(\frac{Q(\theta)}{Q}\right)$ подстановками группы S_8 основывающиеся на:

а) равенствах (11), выражающих присоединяемые к полю Q элементы $\sqrt{2};\sqrt{3};i$ через корень $\theta=\theta_t$ уравнения $f(x)=0$;

б) равенствах (12), выражающих корни $\theta_2;\theta_3;...;\theta_8$ через корень $\theta=\theta_1$ уравнение $f(x)=0$.

Реализуя возможность в), основывающуюся на теореме о продолжении изоморфизмов [2], отметим, что в возрастающей цепочке подполей $Q \prec Q(\sqrt{2}) \prec Q(\sqrt{2};\sqrt{3}) \prec Q(\sqrt{2};\sqrt{3};i)$ степень каждого последующего подполя над непосредственно предшествующим равна 2. Отсюда следует, что группа Галуа каждого подполя над предшествующим состоит из двух элементов (автоморфизмов), при этом:

– поле $Q(\sqrt{2})$ над Q имеет 2 автоморфизма Φ_{11} и Φ_{12}, которые переводят элемент $\sqrt{2}$, как корень неприводимого над Q многочлена x^2-2, в сопряженные с ним над Q элементы $\sqrt{2}$ и $-\sqrt{2}$, соответственно;

– поле $Q(\sqrt{2};\sqrt{3})$ над $Q(\sqrt{2})$ также имеет 2 автоморфизма Φ_{21} и Φ_{22}, которые переводят элемент $\sqrt{3}$, как корень неприводимого над $Q(\sqrt{2})$ многочлена x^2-3, в сопряженные с ним над $Q(\sqrt{2})$ элементы $\sqrt{3}$ и $-\sqrt{3}$, соответственно;

– поле $Q(\sqrt{2};\sqrt{3};i)$, аналогичным образом, имеет над $Q(\sqrt{2};\sqrt{3})$ также имеет 2 автоморфизма Φ_{31} и Φ_{32}, которые переводят элемент i, как корень неприводимого над $Q(\sqrt{2};\sqrt{3})$ многочлена $x^2+1=0$, в сопряженные с ним (над этим подполем) элементы i и $-i$, соответственно.

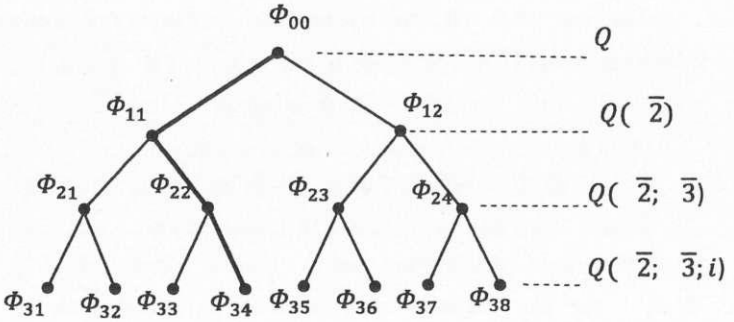


Рисунок 1 – Автоморфизмы группы $G\left(Q(\theta)/Q\right)$

Обозначая через Φ_{00} тождественный автоморфизм основного поля Q, отметим, что автоморфизмы поля $Q(\theta)=Q(\sqrt{2};\sqrt{3};i)$ над полем Q можно получить, как последовательные продолжения этого автоморфизма, в соответствии со следующей схемой (смотри рисунок 1).

Эта схема представляет собой двуветвящееся дерево. Каждой его веточке соответствует автоморфизм поля $Q(\theta)$ над Q. В частности, обозначая автоморфизм, соответствующий выделенной веточке через Φ, получаем, что $\Phi(\sqrt{2})=\Phi_{11}(\sqrt{2})=\sqrt{2}$; $\Phi(\sqrt{3})=\Phi_{22}(\sqrt{2})=-\sqrt{3}$; $\Phi(i)=\Phi_{34}(i)=-i$, т. е.

$$\Phi(\theta_1)=\Phi(\sqrt{2}+\sqrt{3}+i)=\Phi(\sqrt{2})+\Phi(\sqrt{3})+\Phi(i)=\sqrt{2}-\sqrt{3}-i=\theta_7.$$

Следовательно $\Phi=\Phi_7$.

Аналогичным образом находим подстановки группы S_8, соответствующие остальным автоморфизмам группы $G\left(Q\ \theta\ /\ Q\right)$. При этом, если подстановки находятся посредством реализации возможности б), то вычислительную работу можно значительно упростить, используя очевидные соотношения над корнями $\theta_1;\theta_2;...;\theta_8$:

$$\theta_1+\theta_8=0;\ \theta_2+\theta_5=0;\ \theta_3+\theta_7=0;\ \theta_4+\theta_6=0. \qquad (14)$$

Так как $\Phi\ 0\ =0$, то, из первого соотношения совокупности соотношений (14), получаем $\Phi\ \theta_1+\theta_8\ =\Phi\ \theta_1\ +\Phi\ \theta_8\ =0$, т. е.

$$\Phi_i\ \theta_8\ =-\Phi_i\ \theta_1\ .$$

Остальные соотношения, соответственно, дают:

$$\Phi_i\ \theta_5\ =-\Phi_i\ \theta_2\ ;\ \Phi_i\ \theta_7\ =-\Phi_i\ \theta_3\ ;\ \Phi_i\ \theta_6\ =-\Phi_i\ \theta_4\ .$$

Таким образом, в рассматриваемом случае, для нахождения подстановки π_i достаточно найти только образы $\Phi_i\ \theta_2$; $\Phi_i\ \theta_3$; $\Phi_i\ \theta_4$, так как согласно определению автоморфизмов Φ_i имеем $\Phi_i\ \theta_1\ =\theta_i\ \ i=1;2;...;8$.

13. Сведя полученные результаты в единую таблицу, будем иметь (смотри таблицу 2).

Таблица 2 – Представление автоморфизмов группы $G\left(Q\ \theta\ /\ \theta\right)$ подстановками

Φ_i	Подстановка π_i	Разложение π_i в произведение независимых циклов
Φ_1	$\begin{pmatrix}1&2&3&4&5&6&7&8\\1&2&3&4&5&6&7&8\end{pmatrix}$	1 2 3 4 5 6 7 8
Φ_2	$\begin{pmatrix}1&2&3&4&5&6&7&8\\2&1&6&7&8&3&4&5\end{pmatrix}$	12 36 47 58
Φ_3	$\begin{pmatrix}1&2&3&4&5&6&7&8\\3&6&1&5&4&2&8&7\end{pmatrix}$	13 26 45 78
Φ_4	$\begin{pmatrix}1&2&3&4&5&6&7&8\\4&7&5&1&3&8&2&6\end{pmatrix}$	14 27 35 68

Φ_5	$\begin{pmatrix}1&2&3&4&5&6&7&8\\5&8&4&3&1&7&6&2\end{pmatrix}$	15 28 34 67
Φ_6	$\begin{pmatrix}1&2&3&4&5&6&7&8\\6&3&2&8&7&1&5&4\end{pmatrix}$	16 23 48 57
Φ_7	$\begin{pmatrix}1&2&3&4&5&6&7&8\\7&4&8&2&6&5&1&3\end{pmatrix}$	17 24 38 56
Φ_8	$\begin{pmatrix}1&2&3&4&5&6&7&8\\8&5&7&6&2&4&3&1\end{pmatrix}$	18 25 37 46

Таким образом, с точностью до изоморфизма, группа Галуа $G\left(Q\ \theta\ /Q\right)=\left\langle G\left(Q\ \theta\ /Q\right)\ ;\ \cdot\ ;\ \Phi_1\right\rangle$ есть подгруппа

$S_G=\left\langle \pi_i/i=1;2;...;n\ \ ;\ \cdot\ ;\ \pi_1\right\rangle$ симметрической группы S_8.

Используя этот изоморфизм, получаем таблицу Кэли, представляющего операцию $\square$ - композиции гомоморфизмов группы $G\left(Q\ \theta\ /Q\right)$ (смотри таблицу 3).

Таблица 3 – Таблица Кэли • – композиции автоморфизмов

•	Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6	Φ_7	Φ_8
Φ_1	Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6	Φ_7	Φ_8
Φ_2	Φ_2	Φ_1	Φ_6	Φ_7	Φ_8	Φ_3	Φ_4	Φ_5
Φ_3	Φ_3	Φ_6	Φ_1	Φ_5	Φ_4	Φ_2	Φ_8	Φ_7
Φ_4	Φ_4	Φ_7	Φ_5	Φ_1	Φ_3	Φ_8	Φ_2	Φ_6
Φ_5	Φ_5	Φ_8	Φ_4	Φ_3	Φ_1	Φ_7	Φ_6	Φ_2
Φ_6	Φ_6	Φ_3	Φ_2	Φ_8	Φ_7	Φ_1	Φ_5	Φ_4
Φ_7	Φ_7	Φ_4	Φ_8	Φ_2	Φ_6	Φ_5	Φ_1	Φ_3
Φ_8	Φ_8	Φ_5	Φ_7	Φ_6	Φ_2	Φ_4	Φ_3	Φ_1

Переходя к выявлению структуры подгрупп группы $G\left(Q\ \theta\ /_{Q}\right)$ приведем, предварительно, формулировку основной теоремы теории Галуа [2].

Теорема 4. 1) Каждому промежуточному подполю $\mathcal{L}$, $\mathcal{P} \prec \mathcal{L} \prec \mathcal{F}$, соответствует некоторая подгруппа $\mathcal{H}$ группы Галуа $G\ {}^{\mathcal{F}}/_{\mathcal{P}}$, а именно, совокупность тех автоморфизмов из этой группы, которые оставляют на месте все элементы из $\mathcal{L}$.

Поле $\mathcal{L}$ определяется подгруппой $\mathcal{H}$ однозначно; именно, поле $\mathcal{L}$ является совокупностью тех элементов из $\mathcal{F}$; которые «выдерживают» все подстановки из $\mathcal{H}$, т. е. остаются инвариантными при этих подстановках.

Для каждой подгруппы $\mathcal{H}$ группы $G\ {}^{\mathcal{F}}/_{\mathcal{P}}$ можно найти поле $\mathcal{L}$, которое находится с подгруппой $\mathcal{H}$ в только что описанной связи.

Порядок подгруппы $\mathcal{H}$ равен степени поля $\mathcal{F}$ над полем $\mathcal{L}$; индекс подгруппы $\mathcal{H}$ в группе $G\ {}^{\mathcal{F}}/_{\mathcal{P}}$ равен степени поля $\mathcal{L}$ над полем $\mathcal{P}$.

В дальнейшем группу $G\left(Q\ \theta\ /_{Q}\right)$ будем обозначать через G_{16}.

Это обозначение обусловлено тем, что (как это будет показано ниже) группа $G\left(Q\ \theta\ /_{Q}\right)$ содержит, включая несобственные, 16 различных подгрупп и подгруппа $G\left(Q\ \theta\ /_{Q}\right)$ будет наибольшей, по отношению теоретико-множественного включения, среди всех этих подгрупп.

Единичную подгруппу группы G_{16} будем обозначать G_1, т. е. $G_1 = \langle \Phi_1\ ;\ ;\ \Phi_1 \rangle$.

Симметричность таблицы 2 относительно главной диагонали показывает, что группа G_{16} коммутативна.

Порядками собственных подгрупп группы G_{16}, согласно теореме Лагранжа, могут быть только числа 2 и 4. Так как длины циклов, в разложении (соответствующих автоморфизмам Φ_i группы G_{16})

подстановок π_i $i=1;2;...;8$ в произведения независимых циклов, равны 2, то каждый нетождественный автоморфизм Φ_i этой группы порождает подгруппу порядка 2. Обозначая через G_i подгруппу, порожденную автоморфизмом Φ_i $(i=1;2;...;8)$, получаем следующие 7 подгрупп порядка 2 группы G_{16}:

$$G_2=\langle\{\Phi_1;\Phi_2\};\square;\Phi_1\rangle; \qquad G_6=\langle\{\Phi_1;\Phi_6\};\square;\Phi_1\rangle;$$
$$G_3=\langle\{\Phi_1;\Phi_3\};\square;\Phi_1\rangle; \qquad G_7=\langle\{\Phi_1;\Phi_7\};\square;\Phi_1\rangle;$$
$$G_4=\langle\{\Phi_1;\Phi_4\};\square;\Phi_1\rangle; \qquad G_8=\langle\{\Phi_1;\Phi_8\};\square;\Phi_1\rangle.$$
$$G_5=\langle\{\Phi_1;\Phi_5\};\square;\Phi_1\rangle;$$

Любая другая собственная подгруппа группы G_{16} (при условии их существования) должна содержать четыре элемента (автоморфизма) этой группы.

Заметим, что если $\Phi_i;\Phi_j\in G_1$; $i,j\in(2;3;...;8)$ и $i\neq j$, то подгруппа группы G_{16}, порожденная элементами Φ_i и Φ_j, будет подгруппой порядка 4. Действительно, так как $\Phi_i\neq\Phi_1$ и $\Phi_j\neq\Phi_1$, то $\Phi_k=\Phi_i\square\Phi_j\notin\{\Phi_i;\Phi_j\}$. В то же время:

$$\Phi_k\square\Phi_i=(\Phi_i\square\Phi_j)\square\Phi_i=(\Phi_i\square\Phi_i)\square\Phi_j=\Phi_1\square\Phi_j=\Phi_j\in\{\Phi_i;\Phi_j\};$$
$$\Phi_k\square\Phi_j=(\Phi_i\square\Phi_j)\square\Phi_j=\Phi_i\square(\Phi_j\square\Phi_j)=\Phi_i\square\Phi_1=\Phi_i\in\{\Phi_i;\Phi_j\}.$$

Таким образом, четырехэлементное множество $\{\Phi_1;\Phi_i;\Phi_j;\Phi_k\}$ замкнуто относительно операции $\square$ - композиции автоморфизмов и, следовательно, является носителем некоторой четырехэлементной подгруппы группы G_{16}.

Исходя из вышеприведенных соображений, получаем еще семь собственных подгрупп группы G_{16} (порядка 4):

$$G_9=\langle\{\Phi_1;\Phi_2;\Phi_4;\Phi_7\};\square;\Phi_1\rangle; \qquad G_{13}=\langle\{\Phi_1;\Phi_4;\Phi_6;\Phi_8\};\square;\Phi_1\rangle;$$
$$G_{10}=\langle\{\Phi_1;\Phi_2;\Phi_3;\Phi_6\};\square;\Phi_1\rangle; \qquad G_{14}=\langle\{\Phi_1;\Phi_3;\Phi_7;\Phi_8\};\square;\Phi_1\rangle;$$
$$G_{11}=\langle\{\Phi_1;\Phi_3;\Phi_4;\Phi_5\};\square;\Phi_1\rangle; \qquad G_{15}=\langle\{\Phi_1;\Phi_5;\Phi_6;\Phi_7\};\square;\Phi_1\rangle.$$
$$G_{12}=\langle\{\Phi_1;\Phi_2;\Phi_5;\Phi_8\};\square;\Phi_1\rangle;$$

Так как группа G_{16} абелева, то все эти подгруппы являются нормальными подгруппами и любой ряд подгрупп этой группы будет нормальным. В частности, нормальные ряды

$$G_1 \subset G_3 \subset G_{10} \subset G_{16}; \quad (15)$$

$$G_1 \subset G_5 \subset G_{12} \subset G_{16} \quad (16)$$

дают примеры композиционных рядов этой группы, что подтверждает (с позиции теории Галуа) разрешимость уравнения $f(x)=0$.

Полная структура подгрупп группы G_{16}, относительно теоретико-множественного включения, отражена на нижеприведенном графе (смотри рисунок 2).

В частности, выделенные пути этого графа соответствуют композиционным рядам (15) и (16).

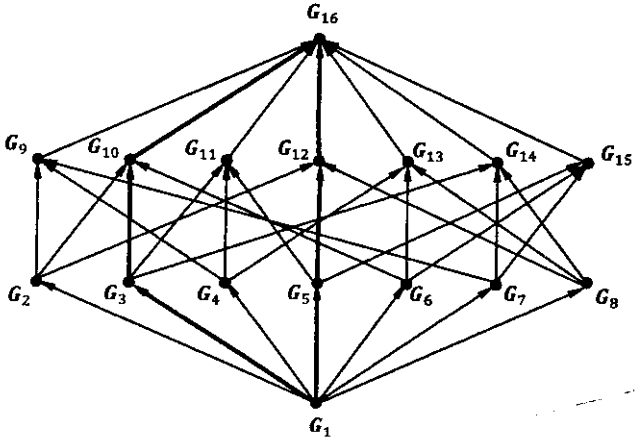


Рисунок 2 – Структура подгрупп группы $G\left(Q(\theta)/Q\right)$

15. Переходя к нахождению подполей поля $Q(\theta)$, соответствующих собственным подгруппам G_2-G_{15} группы $G_{16}=G\left(Q(\theta)/Q\right)$, воспользуемся тем, что элементы $1; \sqrt{2}; \sqrt{3}; \sqrt{6}; i; i\sqrt{2}; i\sqrt{3}; i\sqrt{6}$ соответствуют базису поля $Q(\theta)$, как векторного

пространства, над подполем Q. Присоединение, любого, отличного от 1, элемента этого базис к полю Q приведет к появлению одного из собственных подполей поля $Q(\theta)$. Таким, образом, следуя этому пути, получаем следующие семь подполей поля $Q(\theta)$:

$$Q\ \sqrt{2}\ ;\ Q\ \sqrt{3}\ ;\ Q\ \sqrt{6}\ ;\ Q\ i\ ;\ Q\ i\sqrt{2}\ ;\ Q\ i\sqrt{3}\ ;\ Q\ i\sqrt{6} \qquad (17)$$

Каждое из подполей последовательности (17) является расширением поля Q степени 2, так как степени присоединяемых к Q алгебраических элементов равны 2. В частности, характеристическими многочленами элементов 1; $\sqrt{2}$; $\sqrt{3}$; $\sqrt{6}$; i; $i\sqrt{2}$; $i\sqrt{3}$; $i\sqrt{6}$ является, соответственно, многочлены:

$$x^2-2;\ x^2-3;\ x^2-6;\ x^2+1;\ x^2+2;\ x^2+3;\ x^2+6,$$

неприводимые над полем Q.

В соответствии с основной теоремой теории Галуа, индексы подгрупп, соответствующих подполям последовательности (17) в группе G_{16} должны быть равны 2, т. е. сами эти подгруппы должны быть четырехэлементными подгруппами этой группы.

Используя систему равенств (11), для каждого из элементов 1; $\sqrt{2}$; $\sqrt{3}$; $\sqrt{6}$; i; $i\sqrt{2}$; $i\sqrt{3}$; $i\sqrt{6}$ находим совокупность автоморфизмов группы G_{16}, оставляющих этот элемент на месте.

Найдем, для примера, автоморфизмы, оставляющие на месте элемент $i\sqrt{2}$. Согласно пятому равенству системы равенств (11):

$$i\sqrt{2}=-\frac{13}{8}-\frac{27}{16}\theta_1^2+\frac{9}{32}\theta_1^4-\frac{1}{64}\theta_1^6.$$

Отсюда:

$$\Phi_2\ i\sqrt{2}\ =\Phi_2\left(-\frac{13}{8}-\frac{27}{16}\theta_1^2+\frac{9}{32}\theta_1^4-\frac{1}{64}\theta_1^6\right)=\Phi_2\left(-\frac{13}{8}\right)+\Phi_2\left(-\frac{27}{16}\theta_1^2\right)+$$

$$+\Phi_2\left(\frac{9}{32}\theta_1^4\right)+\Phi_2\left(-\frac{1}{64}\theta_1^6\right)=-\frac{13}{9}-\frac{37}{16}\ \Phi_2\ \theta_1\ ^2+\frac{9}{32}\ \Phi_2\ \theta_1\ ^4-$$

$$-\frac{1}{64}\ \Phi_2\ \theta_1\ ^6=-\frac{13}{9}-\frac{27}{16}\theta_2^2+\frac{9}{32}\theta_2^4-\frac{1}{64}\theta_2^6=-\frac{13}{9}-\frac{27}{16}\ \sqrt{2}+\sqrt{3}-i\ ^2+$$

$$+\frac{9}{32}\ \sqrt{2}+\sqrt{3}-i\ ^4-\frac{1}{64}\ \sqrt{2}+\sqrt{3}-i\ ^6=-\frac{13}{9}-\frac{27}{16}\ 4+2\sqrt{6}-2\sqrt{2}i-2\sqrt{3}i\ +$$

$$+\frac{9}{32}\ 20+8\sqrt{6}-40\sqrt{2}i-32\sqrt{3}i\ -\frac{1}{64}\ -176-72\sqrt{6}-440\sqrt{2}i-360\sqrt{3}i\ =$$

$$=-\frac{13}{9}-\frac{108}{16}+\frac{54}{16}\sqrt{2}i+\frac{54}{16}\sqrt{3}i-\frac{54}{16}\sqrt{6}+\frac{180}{32}-\frac{360}{32}\sqrt{2}i-\frac{288}{32}\sqrt{3}i+\frac{72}{36}\sqrt{6}+$$

$$+\frac{176}{64}+\frac{440}{64}\sqrt{2}i+\frac{360}{64}\sqrt{3}i+\frac{72}{64}\sqrt{6}=\frac{-104-432+360+176}{64}+$$

$$+\frac{216-720+440}{64}\sqrt{2}i+\frac{216-576+360}{64}\sqrt{3}i+\frac{-216+144+72}{64}\sqrt{6}=-i\sqrt{2}.$$

Аналогично находим,

$$\Phi_3\ i\sqrt{2}\ =-\sqrt{2}i;\qquad \Phi_5\ i\sqrt{2}\ =-i\sqrt{2};\qquad \Phi_7\ i\sqrt{2}\ =-i\sqrt{2};$$

$$\Phi_4\ i\sqrt{2}\ =i\sqrt{2};\qquad \Phi_6\ i\sqrt{2}\ =i\sqrt{2};\qquad \Phi_8\ i\sqrt{2}\ =i\sqrt{2}.$$

Учитывая, что Φ_1 - тождественный автоморфизм, получаем, что элемент $i\sqrt{2}$ остается на месте под действием автоморфизмов Φ_1; Φ_4; Φ_6; Φ_8. Оставшиеся автоморфизмы группы G_{16} переводят этот элемент в $-i\sqrt{2}$, т. е. в элемент, сопряженный с $i\sqrt{2}$. Исходя из этого получаем, что подполю $Q\ i\sqrt{2}$ соответствует подгруппа

$G_{13}=\langle\ \Phi_1;\Phi_4;\Phi_6;\Phi_8\ ;\square;\ \Phi_1\rangle$ группы G_{16}.

Подобным же образом находим подгруппы, соответствующие остальным подполям последовательности (17).

Сводя полученные результаты в единую таблицу (смотри таблицу 4), будем иметь следующую картину.

Таблица 4 – Соответствие Галуа (I)

№	Подполе	Соответствующая подгруппа	№	Подполе	Соответствующая подгруппа
1	$Q\ \sqrt{2}$	G_9	5	$Q\ i\sqrt{2}$	G_{13}
2	$Q\ \sqrt{3}$	G_{10}	6	$Q\ i\sqrt{3}$	G_{14}
3	$Q\ i$	G_{11}	7	$Q\ i\sqrt{6}$	G_{15}
4	$Q\ \sqrt{6}$	G_{12}	8	Q	G_{16}

В восьмой строке таблицы 4 стоит поле Q (и группа G_{16}), все элементы которого остаются на месте под действием любого автоморфизма этой группы.

16. Перейдем теперь к нахождению подполей $\mathcal{L}$ $Q \subset \mathcal{L} \subset Q(\theta)$ поля $Q(\theta)$, соответствующих двухэлементным подгруппам группы G_{16}. Вновь, исходя из основной теоремы теории Галуа, получаем, что степень поля $Q(\theta)$ над подполем $\mathcal{L}$ должна быть равна 2, т. е. степень любого такого подполя над полем Q должна быть равна 4. Таким образом, любое из подполей $\mathcal{L}$, о которых говорилось выше, может быть получено последовательным присоединением некоторых элементов α, β из последовательности $1; \sqrt{2}; \sqrt{3}; \sqrt{6}; i; i\sqrt{2}; i\sqrt{3}; i\sqrt{6}$. Заметим, что не всегда присоединение различных пар элементов из этой последовательности дает различные расширения поля Q степени 4. В частности, нетрудно заметить, что $Q(\sqrt{3}; i\sqrt{6}) = Q(\sqrt{3}; i\sqrt{2})$. Действительно,

$$Q(\sqrt{3}; i\sqrt{6}) \subseteq Q(\sqrt{3}; i\sqrt{2}),$$

так как $\sqrt{3} \in Q(\sqrt{3}; i\sqrt{2})$ и $i\sqrt{6} = \sqrt{3} \cdot i\sqrt{2} \in Q(\sqrt{3}; i\sqrt{2})$.

Обратное включение, $Q(\sqrt{3}; i\sqrt{2}) \subseteq Q(\sqrt{3}; i\sqrt{6})$, также является верным, так как $\sqrt{3} \in Q(\sqrt{3}; i\sqrt{6})$ и $i\sqrt{2} = i\sqrt{6} : \sqrt{3} \in Q(\sqrt{3}; i\sqrt{6})$.

Нетрудно проверить, что различные расширения поля Q степени 4 получаются присоединением следующих пар:

$$\sqrt{2}; \sqrt{3}\ ;\ \sqrt{3}; i\ ;\ \sqrt{2}; i\ ;\ \sqrt{6}; i\ ;\ \sqrt{3}; \sqrt{2}i\ ;\ \sqrt{2}; \sqrt{3}i\ ;\ \sqrt{2}i; \sqrt{3}i\ .$$

Это дает еще семь расширений:

$$Q(\sqrt{2}; \sqrt{3})\ ;\quad Q(\sqrt{3}; i)\ ;\quad Q(\sqrt{2}; i)\ ;\quad Q(\sqrt{6}; i)\ ;\quad Q(\sqrt{3}; \sqrt{2}i)\ ;$$

$$Q(\sqrt{2}; \sqrt{3}i)\ ;\ Q(\sqrt{2}i; \sqrt{3}i) \qquad (18)$$

поля Q.

Подгруппы группы G_{16}, соответствующие этим подполям, можно найти аналогично тому, как были найдены подгруппы

соответствующие подполям последовательности (17). Но можно поступить и по другому, воспользовавшись нижеприведенным утверждением.

Предложение 1. Пусть $\mathcal{F}$ - расширение Галуа поля $\mathcal{P}$ и $G\,{}^{\mathcal{F}}\!/_{\mathcal{P}}$ группа Галуа этого расширения. Если $\mathcal{L}_1$ и $\mathcal{L}_2$ два промежуточных подполя, т. е. $\mathcal{P} \subseteq \mathcal{L}_1 \subseteq \mathcal{F}$ и $\mathcal{P} \subseteq \mathcal{L}_2 \subseteq \mathcal{F}$, а $\mathcal{H}_1$ и $\mathcal{H}_2$ - подгруппы, соответствующие подполям $\mathcal{L}_1$ и $\mathcal{L}_2$, то подгруппа $\mathcal{H}_1 \cap \mathcal{H}_2$ соответствует наименьшему подполю поля $\mathcal{F}$, содержащему $\mathcal{L}_1$ и $\mathcal{L}_2$.

Применительно к рассматриваемому случаю, роль полей $\mathcal{P}$ и $\mathcal{F}$ играют, соответственно, поля Q и $Q\ \sqrt{2};\sqrt{3};i$.

Продемонстрируем применение этого предложения на примере нахождения подгруппы, соответствующей подполю $Q\ \sqrt{3};\sqrt{2}i$. В качестве промежуточных подполей $\mathcal{L}_1$ и $\mathcal{L}_2$ будем рассматривать подполя $Q\ \sqrt{3}$ и $Q\ \sqrt{2}i$. Легко понять, что наименьшим подполем, содержащим эти подполя является выбранное подполе $Q\ \sqrt{3};\sqrt{2}i$. Согласно предложению 1, этому подполю будет соответствовать пересечение подгрупп, соответствующих подполям $Q\ \sqrt{3}$ и $Q\ \sqrt{2}i$, т. е. подгрупп G_{10} и G_{13}. Так как

$$G_{10} \cap G_{13} = \Phi_1;\Phi_2;\Phi_3;\Phi_6 \cap \Phi_1;\Phi_4;\Phi_6;\Phi_8 = \Phi_1;\Phi_6 ,$$

то подполю $Q\ \sqrt{3};\sqrt{2}i$ будет соответствовать подгруппа $\left\langle \Phi_1;\Phi_6 \ ; \square ;\Phi_1 \right\rangle$, т. е. подгруппа G_6.

Подобным образом можно найти соответствующие подгруппы для других подполей последовательности (18).

Сведем, как и ранее, полученные результаты в одну таблицу (смотри таблицу 5).

Таблица 5 – Соответствие Галуа (II)

№	Подполе	Соответствующая подгруппа	№	Подполе	Соответствующая подгруппа
9	$Q(\sqrt{2};\sqrt{3})$	G_2	13	$Q(\sqrt{3};\sqrt{2}i)$	G_6
10	$Q(\sqrt{3};i)$	G_3	14	$Q(\sqrt{2};\sqrt{3}i)$	G_7
11	$Q(\sqrt{2};i)$	G_4	15	$Q(\sqrt{2}i;\sqrt{3}i)$	G_8
12	$Q(\sqrt{6};i)$	G_5	16	$Q(\sqrt{2};\sqrt{3};i)$	G_1

В последней (шестнадцатой) строке этой таблицы стоит поле $Q(\sqrt{2};\sqrt{3};i)=Q(\theta)$, которое выдерживает только тождественный автоморфизм. Т. е. подгруппой группы G_{16} соответствующей этому полю, является единичная подгруппа G_1.

17. Полная структура подполей поля $Q(\sqrt{2};\sqrt{3};i)$, относительно теоретико-множественного включения, приведена ниже (смотри рисунок 3). Ориентация ребер орграфов, приведенных на рисунках 2 и 3, показывает, что алгебраические системы $\left\langle \mathfrak{B}G\left(Q(\theta)/Q\right);\subseteq\right\rangle$ и $\left\langle \mathfrak{B}Q(\theta);\subseteq\right\rangle$, где $\mathfrak{B}G\left(Q(\theta)/Q\right)$ - множество всех подгрупп группы $G\left(Q(\theta)/Q\right)$, а $\mathfrak{B}Q(\theta)$ - множество всех подполей поля $Q(\theta)$, являются антиизоморфными. Действительно, отображение $\psi:\mathfrak{B}G\left(Q(\theta)/Q\right)\to\mathfrak{B}Q(\theta)$, определенное соответствием Галуа (смотри таблицы 4 и 5), является биективным и удовлетворяет условию: если $G_i\subset G_j$, то $\psi G_i\supset\psi G_j$ для любых подгрупп G_i; G_j группы $G\left(Q(\theta)/Q\right)$, $i\neq j$, $i;j=1;2;...;16$. В частности, композиционному

ряду $G_1 \subset G_3 \subset G_{10} \subset G_{16}$ подгрупп группы $G\left(Q\ \theta \Big/ Q\right)$ соответствует ряд $Q\ \sqrt{2};\sqrt{3};i\ \supset Q\ \sqrt{3};i\ \supset Q\ \sqrt{3}\ \supset Q$ подполей поля $Q\ \theta$.

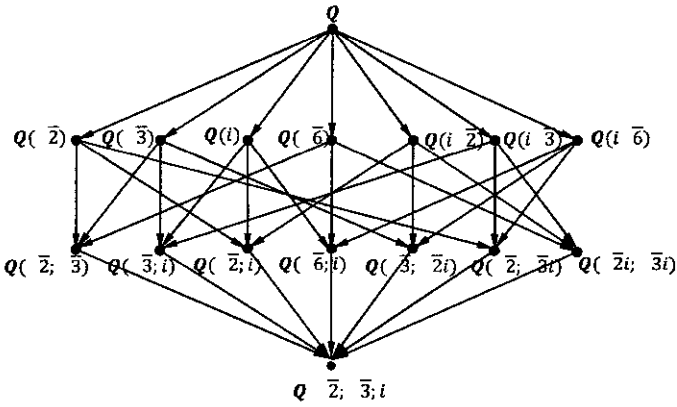


Рисунок 3 – Структура подполей поля $Q\ \sqrt{2};\sqrt{3};i$

СПИСОК ЛИТЕРАТУРЫ

1 **Дроботун, Б. Н., Панасенко, О. И.** Группы Галуа и соответствия Галуа конечных расширений поля рациональных чисел (I). Вестник ПГУ. Серия физико-математическая, №1 – Павлодар, 2013. – 21 с.

2 **Ван дер Варден, Б. Л.** Алгебра. – 2-е издание. – М. : Наука, 1979. – 623 с.

Павлодарский государственный университет
имени С. Торайгырова, Павлодар.
Материал поступил в редакцию 26.03.13.

Б. Н. Дроботун, О. И. Панасенко

Галуа топтары және рационал сандар өрісінің ақырлы кеңей тілулерінің Галуа үйлесімділігі (II)

С. Торайғыров атындағы Павлодар
мемлекеттік университеті, Павлодар қ.
Материал 26.03.13 редакцияға түсті.

B. N. Drobotun, O. I. Panasenko

Galoi's groups and adequacies of final extension of the field of rational numbers (II)

Pavlodar State University named after S. Toraigyrov, Pavlodar.
Material received on 12.06.13.

Жоғары оқу орындарында Галуа теориясының негіздерін меңгеруде әдінамалық әдістерді әзірлеуге арналған берілген жұмыста Галуа топтарының ішкітоптарының құрылымын анықтау технологиясының және осы құрылымдар арысындығы Галуа үйлесімділігін құру әуе рационал сандар өрістерінің (деңгей 2) құрамды алгебралық кеңей тілулерінің ішкі өрістереің сипаттамасы ұсынылады.

In this work devoting to the working out of the methodological ways of the studying foundation of Galoi's theory in the higher establishments the description of the technologies of the revealing of the structures of Galoi's subgroups and subfields of the composite algebraic extension (degree - 2) of the field of rational numbers and construction of Galoi's adequaces between these structures is given.

УДК 512.774.3

Б. Н. Дроботун, Р. С. Садыкова

ПРИНЦИП ДВОЙСТВЕННОСТИ В БУЛЕВЫХ АЛГЕБРАХ

В работе определяется алгебра суперпозиций, как алгебра, носителем которой служит множество всех булевых функций двузначной логики, и в терминах автоморфизмов этой алгебры дается нетрадиционный подход к изучению принципа двойственности для булевых алгебр.

1. Двойственный характер, свойственный явлениям и процессам окружающей действительности, обусловил дихотомичность мышления человека, что нашло свое широкое отражение в категориях

и концептах различных наук, а также в принципах и методах научного (в частности, математического) познания.

Одним из фундаментальных принципов математики является, так называемый, принцип двойственности. Первичные представления об этом принципе, применительно к математике, можно составить следующим образом. В различных разделах математических наук имеются объекты (и понятия об этих объектах) двойственные по отношению друг к другу. К примеру: в порядковых структурах к числу двойственных относятся отношения $\leq$ - «меньше или равно» и $\geq$ - «больше или равно»; в различных геометрических теориях двойственными являются понятия «точка» и «прямая» («прямая» и «плоскость», «сторона» и «угол»); в математической логике - операции & - «конъюнкция» и $\vee$ - «дизъюнкция» и т.п.

В содержательном плане креативная сущность принципа двойственности заключается в том, что если в любом верном предложении того или иного раздела математики заменить все входящие в него понятия на двойственные, то полученное в результате такой замены новое предложение, (т. е. предложение, двойственное к данному), также будет являться верным.

В частности, в евклидовой геометрии на плоскости верным является как утверждение: «Две различные точки определяют единственную прямую», так и двойственное ему утверждение: «Две различные прямые определяют единственную точку», т. е. утверждение, полученное из данного, заменой понятий «точка» и «прямая» на двойственные им понятия «прямая» и «точка», соответственно.

В эллиптической геометрии, где двойственными являются понятия «отрезок» и «угол», одновременно имеют место следующие (двойственные по отношению друг к другу) утверждения:

а) два треугольника равны, если три стороны одного соответственно равны трем сторонам другого;

б) два треугольника равны, если три угла одного соответственно равны трем углам другого.

Глубокое отражение принцип двойственности получил в теории булевых алгебр. Булевы алгебры, как модели определенных

фрагментов человеческого мышления, в наиболее ярких и выразительных формах воплотили в себе его двойственную природу.

В соответствии с этим, принцип двойственности рассматривается нами применительно к алгебре булевых функций, которая является одним из традиционных примеров булевых алгебр.

В предлагаемой работе определяется алгебра суперпозиций, как алгебра, носителем которой служит множество всех булевых функций, и в терминах автоморфизмов этой алгебры дается нетрадиционный подход к изучению данного принципа.

Составляющие понятийно-терминологического аппарата и системы символических обозначений, используемые в работе, являются общепринятыми (смотри, к примеру, [1,2]).

2. Введем ряд понятий, необходимых для дальнейшего изложения работы.

Пусть $E = \{0; 1\}$ и E^n - n-ая декартова степень множества E.

Определение 1. Отображение $f: E^n \to E$ - множества E^n в множество E называется n-местной функцией алгебры логики (или n-местной булевой функцией).

Через $B_2^{(n)}$ обозначим множество всех функций алгебры логики $n \in N$. Положим $B_2 = \overset{\infty}{_{n=0}} B_2^{(n)}$, т. е. B_2 - множество всех функций алгебры логики от любого конечного числа переменных. Если $f \in B_2$, то запись $f = f(x_1; x_2; \ldots; x_n)$ будет означать, что все переменные функции f принадлежат множеству $x_1; x_2; \ldots; x_n$. Если $\sigma \in E$, то $\bar{\sigma} = 0$, если $\sigma = 1$ и $\bar{\sigma} = 1$, если $\sigma = 0$.

Определение 2. Пусть $f \in B_2^{(n)}$ и $f = f(x_1; x_2; \ldots; x_n)$. Функция $f^* = f^*(x_1; x_2; \ldots; x_n)$ называется двойственной к f, если

$$f^*(\sigma_1; \sigma_2; \ldots; \sigma_n) = \bar{f}\ \bar{\sigma}_1; \bar{\sigma}_2; \ldots; \bar{\sigma}_n$$

для любого набора $\sigma^{(n)} = (\sigma_1; \sigma_2; \ldots; \sigma_n) \in E^n$.

Определение 3. Пусть $\varphi \in B_2^{\,n}$, $g_1; g_2; \ldots; g_n \in B_2^{\,m}$ и $\varphi = \varphi(x_1; x_2; \ldots; x_n)$; $g_1 = g_1\ x_1; x_2; \ldots; x_m$; $g_2 = g_2\ x_1; x_2; \ldots; x_m$; ... $g_n = g_n\ x_1; x_2; \ldots; x_m$. Суперпозицией $S^{n,m}(\varphi; g_1; g_2; \ldots; g_n)$ функций $\varphi; g_1; g_2; \ldots; g_n$ называется функция

$$f\ x_1; x_2; \ldots; x_m = \varphi(g_1\ x_1; x_2; \ldots; x_m;\ g_2\ x_1; x_2; \ldots; x_m;\ \ldots; g_n\ x_1; x_2; \ldots; x_m). \quad (1)$$

Определение 3 является естественным обобщением (известного из школьной математики) понятия сложной функции $\varphi\ g\ x$, которая получается из одноместных функций $\varphi(x)$ и $g(x)$ посредством подстановки функции $g(x)$ в функцию $\varphi(x)$ вместо переменной x.

Принцип двойственности для булевых функций в его канонической трактовке формулируется следующим образом: если $f = S^{n;m}\ \varphi; g_1; g_2; \dots g_n$, то $f^* = S^{n;m}\ \varphi^*; g_1^*; g_2^*; \dots g_n^*$ для любых $f: g_1; g_2; \dots g_n \in B_2$. Согласно этому принципу, функция, двойственная суперпозиции функций, является соответствующей суперпозицией двойственных функций.

Напомним доказательство этого принципа [3]. Итак, пусть функция $f\ x_1; x_2; \dots x_m$ является суперпозицией функций $\varphi; g_1; g_2; \dots g_n$, т. е. функцией, полученной из этих функций в соответствии с правилом (1). Тогда:

$$S^{n;m}\ \varphi; g_1; g_2; \dots g_n\ ^* = f^*\ x_1; x_2; \dots x_m\ = f\ x_1; x_2; \dots x_m\ =$$

$$= \varphi\ g_1\ x_1; x_2; \dots x_m\ ;\ g_2\ x_1; x_2; \dots x_m\ ;\ \dots;\ g_n\ x_1; x_2; \dots x_m\ =$$

$$= \varphi\ g_1\ x_1; x_2; \dots x_m\ ;\ g_2\ x_1; x_2; \dots x_m\ ;\ \dots;\ g_n\ x_1; x_2; \dots x_m\ =$$

$$= \varphi\ g_1^*\ x_1; x_2; \dots x_m\ ;\ g_2^*\ x_1; x_2; \dots x_m\ ;\ \dots;\ g_n^*\ x_1; x_2; \dots x_m\ =$$

$$= \varphi^*\ g_1^*\ x_1; x_2; \dots x_m\ ;\ g_2^*\ x_1; x_2; \dots x_m\ ;\ \dots;\ g_n^*\ x_1; x_2; \dots x_m\ =$$

$$= S^{n;m}\ \varphi^*; g_1^*; g_2^*; \dots; g_n^*\ , \qquad (2)$$

Если взять начало и конец цепочки равенств (2), то получим равенство $S^{n;m}\ \varphi; g_1; g_2; \dots g_n\ ^* = S^{n;m}\ \varphi^*; g_1^*; g_2^*; \dots; g_n^*$, аналогичное, по своему формальному строению, условию «сохранения операций» в определении понятия изоморфизма алгебраических систем [1].

Эта аналогия и обусловила возможность определения алгебры суперпозиций, как алгебры, носителем которой является множество B_2- булевых функций, а основными операциями - всюду определенные аналоги суперпозиций этих функций, а также возможность представления принципа двойственности посредством соответствующего автоморфизма этой алгебры.

3. Суперпозицию $S^{n;m}$ можно рассматривать, как частичную $n+1$ -местную операцию, заданную на множестве B_2 функций алгебры логики. Значением этой операции применительно к функциям

$\varphi \in B_2^{(n)}$ и $g_1; g_2; \dots g_n \in B_2^{(m)}$ является булева функция $f = S^{n;m}\ \varphi; g_1; g_2; \dots g_n$. Т. е. условием определенности операции $S^{n;m}$ на наборе $\varphi; g_1; g_2; \dots g_n$ булевых функций является следующее требование: функции g_i должны быть m −местными $i = 1, 2, \dots n$ и число этих функций должно совпадать с местностью n функции ц. В случае нарушения этого условия, значение $S^{n;m}\ \varphi; g_1; g_2; \dots g_n$ будет считаться неопределенным.

Т.к. основные операции алгебраической системы (алгебры) предполагаются алгебраическими, то в качестве всюду определенных аналогов операций $S^{n;m}$ возьмем операции $F^{n;m}$, $m; n \in N$, определенные на B_2 по следующим правилам: $F^{n;m}\ \varphi; g_1; g_2; \dots g_n =$

$$= \begin{cases} S^{n;m}\ \varphi; g_1; g_2; \dots g_n \text{ , если } \varphi \in B_2^{(n)} \text{ и } g_i \in B_2^{(m)}, i = 1, 2, \dots n; \\ \varphi, \text{ в противном случае,} \end{cases} \quad (3)$$

для любых $\varphi; g_i \in B_2,\ i = 1, 2, \dots n$.

Из определения (3) следует, что операции $F^{n;m}$ действительно являются алгебраическими. Это обуславливает возможность определения алгебры

$$\boldsymbol{Sup\, B_2} = \ B_2;\ \ F^{n;m}/n; m \ \in N \quad (4)$$

Алгебру (4) будем называть алгеброй суперпозицией.

Нетрудно видеть, что соответсвие Ф: $B_2 \to B_2$, заданное условием

$$\forall f; g \ \in B_2 \qquad f; g \ \in \Phi \ \Leftrightarrow \ g = f^* \quad (5)$$

является отображением B_2 на B_2. Действительно, $Dom\Phi = B_2$ и сечение соответствия Ф по любому элементу $f \in B_2$ содержит, в силу единственности двойственной к f функции f^*, только один элемент f^*. Т.к. функция f^*, двойственная к f, определяется однозначно и $f^{*\,*} = f$, то Ф является биективным отображением B_2 на B_2. Таким образом, Ф $f\ = f^*$ для любой функции $f \in B_2$.

Предложение 1. Соответствие Ф: $B_2 \to B_2$, определенное по правилу (5) является автоморфизмом алгебры $\boldsymbol{Sup\, B_2}$.

Доказательство. Ранее было отмечено, что соответствие Ф, заданное правилом (5) является биективным отображением B_2на B_2. Осталось убедиться в том, что это отображение сохраняет операции.

Действительно, пусть условие определенности операции $S^{n;m}$ на наборе $\varphi; g_1; g_2; \dots g_n$ выполняется, т. е. $\varphi \in B_2^{(n)}$ и $g_1; g_2; \dots g_n \in B_2^{(m)}$. Тогда, согласно определению операций $F^{n;m}$, будем иметь:

$$\Phi\ F^{n;m}\ \varphi; g_1; g_2; \dots g_n = \Phi\ S^{n;m}\ \varphi; g_1; g_2; \dots g_n =$$
$$= S^{n;m}\ \varphi; g_1; g_2; \dots g_n\ ^* = S^{n;m}\ \varphi^*; g_1{}^*; g_2{}^*; \dots g_n{}^* =$$
$$= F^{n;m}\ \varphi^*; g_1{}^*; g_2{}^*; \dots g_n{}^* = F^{n;m}\ \Phi\ \varphi\ ; \Phi\ g_1\ ; \Phi\ g_2\ ; \dots \Phi\ g_n\ . (6)$$

Из цепочки равенств (6), получаем равенство:

$$\Phi\ F^{n;m}\ \varphi; g_1; g_2; \dots g_n = F^{n;m}\ \Phi\ \varphi\ ; \Phi\ g_1\ ; \Phi\ g_2\ ; \dots \Phi\ g_n\ ,$$

подтверждающее сохранность операции $F^{n;m}$, $n; m \in N$. Если же условие определенности операции $S^{n;m}$ на наборе $\varphi; g_1; g_2; \dots g_n$ не выполняется, то $F^{n;m}\ \varphi; g_1; g_2; \dots g_n = \varphi$, согласно правилу (3). Следовательно, $\Phi\ F^{n;m}\ \varphi; g_1; g_2; \dots g_n = \Phi\ \varphi = \varphi^*$. С другой стороны, будем иметь: $F^{n;m}\ \Phi\ \varphi\ ; \Phi\ g_1\ ; \Phi\ g_2\ ; \dots \Phi\ g_n =$ $= F^{n;m}\ \varphi^*; g_1{}^*; g_2{}^*; \dots g_n{}^* = \varphi^*$, т.к. условие определенности операции $S^{n;m}$на наборе $\varphi^*; g_1{}^*; g_2{}^*; \dots g_n{}^*$ так же, как на наборе $\varphi; g_1; g_2; \dots g_n$, не будет выполняться. Отсюда получаем, что

$$\Phi\ F^{n;m}\ \varphi; g_1; g_2; \dots g_n = F^{n;m}\ \Phi\ \varphi\ ; \Phi\ g_1\ ; \Phi\ g_2\ ; \dots \Phi\ g_n\ .$$

4. Определим на двухэлементном множестве $E = 0; 1$ логические операции; $\vee; \&; \bar{}$ в соответствии с таблицами истинности для формул $x \vee y\ ; (x \& y); \bar{x}$ алгебры высказываний. Очевидно, что полученные операции будут алгебраическими на множестве E. Все это позволяет определить алгебру $\boldsymbol{E} = E; \vee; \&; \bar{}\ ; 0; 1$ сигнатуры $\sigma = F_1{}^2; F_2{}^2; F_3{}^2; c_1; c_2$, если считать, что интерпретация φ сигнатуры σ задается по правилам:

$$\varphi\ F_1{}^2 = \vee; \varphi\ F_2{}^2 = \&; \varphi\ F_3{}^2 = \bar{}\ ; \varphi\ c_1 = 0; \varphi\ c_1 = 1.$$

Нетрудно проверить, что система $\boldsymbol{E}$ является булевой алгеброй и что термальными операциями сигнатуры σ этой алгебры исчерпывающая все формулы алгебры высказываний, логические операции и выделенные элементы которых содержатся в множествах $\vee; \&; \bar{}$ и $0; 1$, соответственно. Проделаем соответствующую проверку для второй части этого утверждения.

С этой целью конкретизируем определение терма сигнатуры σ над множеством предметных переменных $X = x_1; x_2; \dots; x_n; \dots$.

В качестве метасимволов для обозначения переменных из множества X будем использовать символы $x; y; z$ или эти же символы с индексами $x_{i_1}; x_{i_2}; \dots; x_{i_n}; \dots$.

Определение терма носит индуктивный характер:

а) **базис индукции** (шаг 0). Константы c_1 и c_2 сигнатуры σ и любая переменная $x_i \in X$ $(i \in N)$ являются термами этой сигнатуры. Эти термы называются термами шага 0.

б) **индукционное предположение** (шаг k). Предположим, что все термы шагов 0; 1; 2; ...; k уже определены;

в) **индукционный шаг** (шаг$(k+1)$). Пусть $t_1; t_2; t$-произвольные термы, определенные на шагах, номера которых не превосходят k. Тогда все термы шага k и слова $F_1^{\,2}\ t_1; t_2$; $F_2^{\,2}\ t_1; t_2$; $F_3^{\,1}\ t$ являются термами шага $k+1$.

Согласно этому определению любой терм шага k является термом шага $k' > k$. Т. е. если через T_k обозначить множество всех термов шага k, то будем иметь:

$$T_0 \subseteq T_1 \subseteq \cdots \subseteq T_k \subseteq T_{k+1} \subseteq \qquad (7)$$

Таким образом, множество $Term_\sigma(X)$ - всех термов сигнатуры σ есть объединение множеств T_k цепочки (7): $Term_\sigma\ U\ =\ \overset{\infty}{k=0}\ T_k$.

Под сложностью $S(T)$ терма $t \in Term_\sigma(X)$ будем понимать номер шага, на котором этот терм впервые появился в индукционном процессе построения множества $Term_\sigma\ X$. В соответствии с индукционным шагом определения терма, имеют место следующие равенства:

$$S\ \ F_i^{\,2}\ t_1; t_2\ \ = max\ S\ t_1\ ; S\ t_2\ \ + 1,\ i = 1{,}2\ , \qquad (8)$$

$$S\ \ F_3^{\,1}\ t_1\ \ = S\ t\ + 1. \qquad (9)$$

Определение термальной операции $^{\varphi}t$ алгебры $\boldsymbol{E}$, соответствующей терму $t = t(x_1; x_2; \dots x_n) \in Term_\sigma\ X$, дается теперь индукцией по сложности $S\ t$ этого терма:

а) **базис индукции** $S\ t\ = 0$. В этом случае, для терма t могут иметь место следующие возможности:

а.1) $t(x_1; x_2; \dots x_n) = x_i,\ 1 \le i \le n$;

а.2) $t(x_1; x_2; \dots x_n) = c_j,\ j = 1; 2$.

При реализации первой возможности полагаем ${}^{\varphi}t = {}^{\varphi}t(x_1; x_2; \dots x_n) = x_i$, при реализации второй - ${}^{\varphi}t = 0$, если $j = 1$ и ${}^{\varphi}t = 1$, если $j = 2$.

б) **индукционное предположение** $S\ t\ \leq k$. Предположим, что для любого терма t сигнатуры σ, сложность которого не превосходит k, термальная операция t' уже определена.

в) **индукционный шаг** $S\ t\ = k + 1$. В этом случае, в соответствии с индукционным определением терма, для терма t могут иметь место такие возможности:

в. 1) $t = F_i^{\,2}\ t_1; t_2\ ,\ i = 1,2\ ;$

в. 2) $t = F_3^{\,1}\ t'\ ,$

для некоторых термов $t_1; t_2; t'$ сигнатуры σ, сложность которых не превосходит k (смотри соотношения (8), (9)). Тогда, при реализации этих возможностей полагаем, соответственно:

$${}^{\varphi}t = \begin{cases} {}^{\varphi}t_1 \vee {}^{\varphi}t_2\ , \text{ если } i = 1, \\ {}^{\varphi}t_1 \& {}^{\varphi}t_2\ , \text{ если } i = 2; \end{cases} \qquad {}^{\varphi}t = \neg\, {}^{\varphi}t'.$$

Заметим, что эти определения корректны, т.к. термальные операции ${}^{\varphi}t_1,\ {}^{\varphi}t_2,\ {}^{\varphi}t'$, согласно индукционному предположению уже получены.

Из вышеприведенного определения термальной операции следует, что для любого терма $t \in Term_{\sigma}(X)$, выражение ${}^{\varphi}t$ есть формула алгебры высказываний, построенная из переменных множества X посредством конечного числа последовательных применений операций $\vee$; & и $\bar{}$.

Обратная процедура, т. е. процедура получения по любой формуле $\boldsymbol{A} = \boldsymbol{A}\ x_1; x_2; \dots, x_n$ алгебры высказываний, содержащей только операции $\vee$; & и $\bar{}$, соответствующего терма $t_{\boldsymbol{A}}$ осуществляется аналогичным образом индукцией по сложности этой формулы.

5. Будем говорить, что формула $\boldsymbol{A} = \boldsymbol{A}\ x_1; x_2; \dots, x_n$ алгебры высказываний представляет булеву функцию $f = f(x_1; x_2; \dots; x_n)$ (или функция f представима формулой $\boldsymbol{A}$), если $\boldsymbol{A}$ и f имеют одну и ту же таблицу истинности.

Теорема о функциональной полноте для булевых функций [3] утверждает, что для любой булевой функции f найдется формула $\boldsymbol{A}_f$

алгебры высказываний, представляющая эту функцию, причем формулу A_f всегда можно найти среди множества формул алгебры высказываний, содержащих только логические операции $\vee$; $\&$; $\bar{}$ и выделенные элементы 0; 1. С учетом вышеприведенного описания формул этого множества, как термальных операций булевой алгебры $\boldsymbol{E}$, теорему о функциональной полноте можно переформулировать следующим образом; любая булева функция f представима посредством термальной операции A_f алгебры $\boldsymbol{E}$.

В качестве следствия из предложения 1 получим доказательство известного утверждения теории двойственности для булевых функций.

Предложение 2. Если булева функция f представима посредством формулы A_f, как термальной операции алгебры $\boldsymbol{E}$, то для получения формулы A_{f^*}, представляющей двойственную к f функцию f^*, нужно в формуле A_f заменить все вхождения:

0 на 1; 1 на 0; $\vee$ на $\&$ и $\&$ на $\vee$.

Доказательство. Применим индукцию по сложности формулы $A_f = A_f\ x_1; x_2; \ldots, x_n$.

а) **базис индукции** $(S(A_f) = 0)$. В этом случае для формулы A_f, согласно определению термальной операции системы $\boldsymbol{E}$, могут иметь место следующие возможности:

а.1) $A_f = A_f\ x_1; x_2; \ldots, x_n = x_i$;

а.2) $A_f = A_f\ x_1; x_2; \ldots, x_n = 0$;

а.3) $A_f = A_f\ x_1; x_2; \ldots, x_n = 1$.

Т.к. в соответствии с определением формулы, представляющей булеву функцию, A_f и f имеют одинаковые таблицы истинности, то при реализации возможности:

а.1) формула A_f представляет функцию, тождественно равную i-ой переменной, т. е. булеву функцию $f\ x_1; x_2; \ldots; x_n = x_i$;

а.2) формула A_f представляет функцию-константу 0, т. е. булеву функцию $f\ x_1; x_2; \ldots; x_n = 0$;

а.3) формула A_f представляет функцию-константу 1, т. е. булеву функцию $f\ x_1; x_2; \ldots; x_n = 1$.

Найдем функцию $f^* = f^*\ x_1; x_2; \ldots; x_n$ при реализации каждой из этих возможностей:

а.1) согласно определению двойственной функции (смотри определение 2), $f^*(x_1; x_2; \ldots; x_n) = f(x_1; x_2; \ldots; \overline{x_i}; \ldots, x_n) = \overline{x_i} = x_i$, т. е. $A_{f^*} = x_i$;

а.2) т.к. $f(x_1; x_2; \ldots; x_n)$ - функция-константа 0, то ее значение не зависит от значений переменных $x_1; x_2; \ldots; x_n$, из множества Е т. е. $f(x_1; x_2; \ldots; \overline{x_i}; \ldots, x_n) = 0$ и, следовательно, $f^*(x_1; x_2; \ldots; x_n) = f(x_1; x_2; \ldots; \overline{x_i}; \ldots, x_n) = 0 = 1$, т. е. $A_{f^*} = 1$;

а.3) аналогично возможности а.2) получаем, $f^*(x_1; x_2; \ldots; x_n) == f(x_1; x_2; \ldots; \overline{x_i}; \ldots, x_n) = 1 = 0$, т. е. $A_{f^*} = 0$.

Таким образом, в каждом из возможных случаев, имеющих место для формулы A_f сложности 0, доказываемое предложение является верным. При этом при реализации возможности а.1) имеет место равенство $A_f = A_{f^*}$, т.к. в A_f не входит ни одна из операций $\vee$; $\&$; $\overline{\ }$ и ни один из выделенных элементов 0; 1.

б) **индукционное предположение** $S(B) \leq k$. Пусть для любой формулы $B = B_g(x_1; x_2; \ldots; x_n)$, как термальной операции алгебры E, представляющей булеву функцию $g = g(x_1; x_2; \ldots; x_n)$, доказываемое предложение является верным, т. е. для получения формулы $B_{g^*} = B_{g^*}(x_1; x_2; \ldots; x_n)$ (представляющей функцию $g^* = g^*(x_1; x_2; \ldots; x_n)$) из формулы B_g, достаточно произвести в этой формуле указанные замены.

в) **индукционный шаг** $S(A_f) = k + 1$. Покажем, что и для любой формулы $A_f = A_f(x_1; x_2; \ldots, x_n)$, сложность которой равна $k + 1$, доказываемое предложение также является верным. В соответствии с индукционным шагом определения термальной операции, для формулы A_f, в этом случае, могут иметь место следующие возможности:

в.1) $A_f = B_{g_1} \vee B_{g_2}$;

в.2) $A_f = B_{g_1} \& B_{g_2}$;

в.3) $A_f = B_g$.

Покажем, что при реализации любой из этих возможностей, формула A_{f^*} получается из формулы A_f по указанным в предложении правилам.

в.1) Т.к. из $A_f = B_{g_1} \vee B_{g_2}$ следует, что $f(x_1; x_2; \ldots; x_n) = g_1(x_1; x_2; \ldots; x_n) \vee g_2(x_1; x_2; \ldots; x_n)$ то, полагая, $\varphi(x_1; x_2) = x_1 \vee x_2$, будем иметь $f = S^{2;n}(\varphi; g_1; g_2)$. Отсюда, используя предложение 1, получаем $\Phi f = S^{2;n}(\Phi\varphi; \Phi g_1; \Phi g_2)$, где Φ – автоморфизм алгебры $Sup\, B_2$, определенный в этом предложении, т.е.:

$$f^* = S^{2;n}(\varphi^*; g_1^*; g_2^*) \quad (10)$$

Т.к. $\varphi^*(x_1; x_2) = \varphi(x_1; x_2) = x_1 \vee x_2 = x_1 \& x_2$, то из равенства (10) получаем, что $f^* = g_1^* \& g_2^*$, т. е.

$$A_{f^*} = A_{g_1^* \& g_2^*}(x_1; \ldots, x_n) = (B_{g_1^*}(x_1; \ldots; x_n) \& B_{g_2^*}(x_1; \ldots; x_n)) . \quad (11)$$

Из того, что $S(A_f) = k + 1$, с учетом равенства (8) будем иметь: $S(B_{g_1}) \leq k$ и $S(B_{g_2}) \leq k$, т.е., согласно индукционному предположению, формулы $B_{g_1^*}$ и $B_{g_2^*}$ получаются, соответственно, из формул B_{g_1} и B_{g_2} посредством замены всех вхождений 0 на 1; 1 на 0; $\vee$ на & и & на $\vee$. Но тогда, как показывает равенство (11), и формула A_{f^*} получается из формулы $A_f = B_{g_1} \vee B_{g_2}$ посредством аналогичных замен.

в.2); в.3) Доказательства предложения в этих случаях, подобны его доказательству в случае в.1).

СПИСОК ЛИТЕРАТУРЫ

1 **Мальцев, А.И.** Алгебраические системы. - М. : Наука, 1970. – 392 с.

2 **Гончаров, С.С.** Счетные булевы алгебры и разрешимость. – Новосибирск : Научная книга, 1996. – 364 с.

3 **Яблонский, С.В.** Введение в дискретную математику. – М. : Наука, 1979. – 272 с.

Павлодарский государственный университет
имени С. Торайгырова, Павлодар.
Материал поступил в редакцию 20.03.13.

Б. Н. Дроботун, Р. С. Садыкова

Буль алгебрасындағы сынарлас принципі

С. Торайғыров атындағы Павлодар
мемлекеттік университеті, Павлодар қ.
Материал 20.03.13 редакцияға түсті.

B. N. Drobotun, R. S. Sadykova
The principle of duality in Boole`s algebras
Pavlodar State University named after S. Toraigyrov, Pavlodar.
Material received on 20.03.13.

Жұмыста суперпозиция алгебрасы, екімәнді логикасындағы барлық Буль функцияларының жиыны қызметін атқаратын алгебра анықталады, және осы алгебраның автоморфизм терминдерінде Буль алгебраларында сыңарлас принципі зерделеуге дәстүрлі емес тәсілдеме беріледі.

In work the algebra of superpositions as the algebra as which carrier the set of all Boolean functions of two-digit logic serves, and in terms of automorphisms of this algebra is given nonconventional approach to studying of the principle of a duality for Boolean algebras is defined.

УДК 681.3.07

Б. Н. Дроботун, Г. А. Сарсембаева

КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ (I)

Данная статья является первой частью работы, посвященной технологиям шифрования с открытым ключом. В этой статье приводятся описание и доказательное обоснование корректности алгоритмов, применяемых при построении криптосистем с открытым ключом.

1. Введение. Беспрецедентные темпы развития компьютерных систем и возможности их взаимодействия посредством компьютерных сетей определяют все большую зависимость человечества от информации, которая хранится в таких системах и передается по этим сетям. Повсеместное использование электронных средств связи,

обусловив наступление информационной цивилизации, в качестве неизбежных негативных последствий ее становления, породило армию хакеров, активизировало разработку компьютерных вирусов и устройств электронного прослушивания и электронного мошенничества. В связи с этим, все более актуальной становится необходимость создания специальных средств, обеспечивающих защиту информацию от несанкционированного доступа и гарантирующих достоверность сообщений, получаемых по электронным сетям. Как отмечается в работе [1]:

«Современное киберпространство становится местом драматической интеллектуальной битвы, в которой сталкиваются корпоративные интересы многочисленных групп и отдельных личностей. В логическом мире электронных коммуникаций создаются величайшие интеллектуальные шедевры и изощренные средства для их уничтожения. Сама информация превращается в объект, на защиту которого направлены основные усилия и ресурсы многомиллионной армии математиков, программистов, электронщиков и инженеров» [1, с.15].

Важнейшим средством защиты сетей и электронных коммуникаций от различного рода несанкционированных вмешательств является шифрование с открытым ключом. Криптография с ключом общего доступа относится к одному из самых выдающихся достижений компьютерной науки XX века, что обусловило включение элементов криптографии, связанных с возможностями ее применения для защиты информации и электронных сетей от угроз несанкционированного доступа, в программы учебных дисциплин «Дискретная математика» и «Дискретная математика и математическая логика», как базовых дисциплин, входящих в учебные планы ВУЗов для обучения по специальностям «Информационные системы», «Вычислительная техника и программное обеспечение» и многим другим специальностям.

В данной работе, представляющей собой цикл из двух статей, предлагается доступное для широкой аудитории описание алгоритмов, применяемых при построении криптосистем с открытым ключом, приводится их полное математическое обоснование и разрабатывается конкретная криптосистема, позволяющая кодировать (и декодировать) сообщения, записанные в алфавитах естественных языков.

Построенные в работе примеры непосредственного использования этой системы показывают, что она допускает достаточно простую компьютерную реализацию и вполне может быть применена на практике.

Тем не менее, следует отметить, что одним из основных предназначений предложенной криптосистемы, является демонстрация нетрадиционных (и в достаточной степени удивительных) прикладных возможностей теории чисел. Тем самым, при ее построении авторы руководствовались еще и следующими соображениями, приведенными в работе [2]:

«Проблема заинтересованности студентов в изучении той или иной дисциплины неизбежно встает перед каждым преподавателей. В позитивном решении этой проблемы немаловажную роль играют прикладные возможности изучаемой дисциплины. При этом важно не просто указать на область применения теоретических результатов, а посредством конкретных примеров прикладного характера продемонстрировать ее реальные возможности.» [2,с.77].

Таким образом, результаты данной работы, представляя (сами по себе) определенные интерес, могут найти применение в процессе обучения в ВУЗах по специальностям «Прикладная математика», «Вычислительная техника и программирование» и другим инженерным специальностям.

2. Алгоритмы построения открытого и закрытого ключей криптосистемы. История криптографии показывает, что от ее зарождения вплоть до 80-х годов 20-го столетия (период традиционного шифрования) практически все системы шифрования основывались на использовании элементарных возможностей перестановок и подстановок символов алфавитов сообщений, которые осуществлялись по определенным правилам. Совокупность этих правил составляла ключ криптосистемы. Этим ключом, который (естественно) являлся закрытым (секретным), пользовались как отправители сообщений для их предварительного шифрования, так и получатели этих сообщений для их расшифровки. В связи с этим традиционное шифрование получило название симметрического.

Алгоритмы построения криптосистемы с открытым ключом базируются на использовании результатов теории чисел, в частности,

на применении алгебраических и алгоритмических свойств модулярной арифметики. Шифрование с открытым ключом предполагает, в отличие от традиционного шифрования, использование двух различных ключей. Один из них является открытым и может быть сообщен всем желающим отправить шифрованное сообщение. Другой же ключ, используемый для расшифрования, является закрытым (секретным, личным) ключом получателя шифрованных сообщений. В связи с наличием двух различных ключей криптосистемы с открытым ключом называются ассиметрическими.

Как отмечалось выше, технологии шифрования с открытым ключом существенным образом основываются на использовании теоретико-числовых конструкций модулярной арифметики. Открытый и закрытый ключи криптосистемы являются основными составляющими этой системы.

Для их построения:

а) выбираются простые натуральные числа p и q (эти числа относятся к закрытым параметрам криптосистемы, т. е. являются секретными);

б) по выбранным простым числам p и q вычисляется число $n = p \cdot q$ (это число является открытым, т. е. несекретным);

в) находится нечетное натуральное число e, взаимно простое с числом $\varphi(n) = (p-1)\cdot(q-1)$ (число e является открытым, т. е. несекретным и выбирается из целых положительных чисел, меньших $\varphi(n)$, при этом, в качестве e, выбираются, как правило, небольшие числа, удовлетворяющие вышеприведенным условиям (здесь $\varphi = \varphi(x)$ - функция Эйлера);

г) находится число d, которое является закрытым (секретным) и вычисляется по формуле $d = e^{-1}(\mathrm{mod}\,\varphi(n))$ (т. е. число d является решением сравнения $ed \equiv 1(\mathrm{mod}\,\varphi(n))$, при этом в качестве d берется наименьший неотрицательный вычет по модулю $\varphi(n)$.

Открытый ключ $\{n; e\}$ отправителя шифрованных сообщений составляется теперь из чисел n и e. Закрытый (личный, секретный) ключ $\{d; n\}$ получателя этих сообщений составляется из чисел d и n.

Ключи $\{n;e\}$ и $\{d;n\}$ в совокупности и образуют криптосистему $<\{n;e\};\{d;n\}>$ с открытым ключом $\{n;e\}$.

Приведем ряд замечаний по поводу вышеприведенных пунктов а) – г). Прежде всего отметим, что теоретически, зная открытый ключ, можно найти и закрытый (секретный) ключ, т.е., говоря на языке хакеров «взломать криптосистему». Действительно:

1. Т.к. число n является открытым, то разложив его на два простых множителя, можно найти числа p и q (которые раннее были отнесены к секретным);

2. Зная числа p и q, находим число $\varphi(n)=(p-1)\cdot(q-1)$;

3. По числу $\varphi(n)$ находим возможные значения числа e;

4. По возможным значениям чисел e и числу $\varphi(n)$ находим соответствующие возможные значения числа $d=e^{-1}(\mathrm{mod}\,\varphi(n))$;

5. Определив возможные значения d, находим конечное число возможных значений $\{d;n\}$ секретного ключа;

6. Методом «проб и ошибок» выбираем из этих возможных значений для $\{d;n\}$ требуемый секретный ключ.

Т. е. с теоретической точки зрения, криптосистема с открытым ключом может быть признана несовершенной. Но, теоретические возможности далеко не в полной мере адекватны возможностям их практической реализации. Не вдаваясь в подробности практической компьютерной реализации алгоритма разложения числа n на простые множители, отметим, что в настоящее время (при построении криптосистемы с открытым ключом) значения для простых чисел p и q выбираются из диапазона от 10^{75} до 10^{100}. При таком выборе чисел p и q, задача их нахождения по открытому числу n, посредством разложения этого числа на два простых множителя, становится практически невыполнимой даже при использовании (для ее решения) сверхмощной современной компьютерной индустрии.

В частности, создатели криптосистемы PSA (с открытым ключом) Рон Ривест, Ади Шамир и Леонард Адлеман «…воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но

разложение на множители произведения двух таких чисел практически не выполнимо» [3, с. 35]

Для демонстрации работы предлагаемой криптосистемы PSA ее создатели в качестве открытых ключей выбрали следующие значения параметров e и n:

$e = 9007$;

n=1143816257578888676692357799761466120102182967212423625626518429357069352457338978305971235639587050589890751475992900268795435 41.

Разложить вышеприведенное число n на два простых множителя практически невозможно.

3. Технология применения криптосистемы с открытым ключом. Перейдем к описанию технологии применения криптосистемы $<\{n;e\};\{d;n\}>$.

Текст сообщения записывается отправителем в алфавите $A = \{0;1\}$, т. е. представляет собой двоичную последовательность $X = <\delta_1;\delta_2;...;\delta_t>$, где $\delta_i \in \{0;1\}, i = 1;2;...;t$.

Перед шифрованием последовательность X разбивается на блоки одной и той же длины таким образом, чтобы каждый из этих блоков являлся двоичной записью натурального числа M, не превосходящего n. На практике длина блока выбирается равной числу k, которое однозначно определяется по числу n из условия:

$$2^k < n \le 2^{k+1}, \qquad (1)$$

(напомним, что число n - первая составляющая открытого ключа $\{n;e\}$).

Разбиение последовательности X на блоки длины k осуществляется справа - налево. При этом, если последний (т. е. самый левый) блок будет иметь меньшую, чем k длину l, то дополняем его до блока длины k, приписывая слева $k - l$ нулей.

Каждое такое число M шифруется натуральным числом C, удовлетворяющим условию $C \equiv M^e (\mathrm{mod} n)$, где e - вторая составляющая открытого ключа $\{n;e\}$ и в качестве конкретных значений для C выбираются наименьшие неотрицательные вычеты из соответствующих классов вычетов по модулю n. Отметим, что числа C, согласно правилу их выбора, не превосходят n, что гарантирует

возможность получения двоичной записи всех этих чисел в виде двоичной последовательности длины k.

Далее, полученные натуральные числа C переводятся в двоичную систему счисления и из двоичных записей этих чисел отправителем формируется новая двоичная последовательность X', представляющая собой исходное сообщение X в зашифрованном виде. При этом, двоичные блоки длины k, представляющие числа C, записываются в том же порядке, что и двоичные блоки, представляющие соответствующие им числа M.

Адресат, получив зашифрованное сообщение X', по числу n личного кода находит, исходя из условия (1), длину k блока разбиения и разбивает (справа - налево) последовательность X' на блоки длины k. По каждому из полученных блоков, как двоичной записи натурального числа, он восстанавливает соответствующее число C и осуществляет его дешифровку по формуле $M = C^d (\mathrm{mod} n)$, где d - вторая составляющая личного (секретного) кода получателя, при этом в качестве конкретных значений для M вновь выбираются наименьшие неотрицательные вычеты из соответствующих классов вычетов по модулю n. Получив числа M и переводя их в двоичную систему счисления, он из полученных двоичных блоков длины k формирует, располагая их в том же порядке, исходное сообщение X.

4. Обоснование корректности криптосистем. Перейдем теперь к доказательному обоснованию корректности применения криптосистемы $< \{n;e\};\{d;n\} >$, описанной в пункте 3.

Предварительно напомним ряд результатов модулярной арифметики, которые будут использоваться при этом обосновании [5-6].

Предложение 1. Пусть $n \in N$, "$\equiv (\mathrm{mod} n)$"- отношение сравнимости по модулю n и $a,b \in Z$. Тогда:

1. а) Отношение "$\equiv (\mathrm{mod} n)$" обладает свойствами рефлексивности, симметричности и транзитивности, т. е. является отношением эквивалентности;

1. б) Если $a \equiv b(\mathrm{mod} n)$, то $ma \equiv mb(\mathrm{mod} n)$ для любого $m \in Z$, т. е. обе части сравнения можно умножать на одно и то же целое число;

1. в) Если $a \equiv b(\mathrm{mod}n)$, то $a^k \equiv b^k(\mathrm{mod}n)$ для любого $k \in N$, т. е. обе части сравнения можно возводить в степень (с целым положительным показателем);

1. г) $a \equiv b(\mathrm{mod}n)$, тогда и только тогда, когда $b = a + n \cdot t$ для некоторого $t \in Z$, т. е. $a(\mathrm{mod}n) = \{a + nt / t \in Z\}$;

Если $(a;n) = 1$ и $\varphi(x)$- функция Эйлера [4], то $a^{\varphi(n)} \equiv 1(\mathrm{mod}n)$- **теорема Эйлера**;

Функция Эйлера $\varphi(x)$ является мультипликативной, т. е. если $n = r \cdot s$, для некоторых $r; s \in N$ и числа r и s- взаимно просты $((r;s) = 1)$, то

$\varphi(n) = \varphi(r) \cdot \varphi(s)$.

Предложение 2. Пусть $<\{n;e\};\{d;n\}>$ - криптосистемы с открытым ключом $\{n;e\}$. Тогда $M^{\varphi(n)} \equiv M(\mathrm{mod}n)$ для любого натурального числа M, меньшего n.

Доказательство. Т.к. M - натурального число, меньшее n, то для этого числа могут иметь место две возможности:

Числа M и n - взаимно просты $((M;n) = 1)$;

Числа M и n - не взаимно просты $((M;n) \neq 1)$.

Рассмотрим каждую из этих возможностей.

а) Т.к. $(M;n) = 1$, то $M^{\varphi(n)} \equiv 1(\mathrm{mod}n)$ по теореме Эйлера (предложение 1, пункт 2)). Умножив обе части этого сравнения на M, получим, что $M^{\varphi(n)+1} \equiv M(\mathrm{mod}n)$ (предложение 1, пункт 1.б)).

б) Т.к. $n = p \cdot q$ и числа p и q являются простыми, то для каждого числа M, удовлетворяющего условию $1 \leq M < n$, имеет место один и только один из случаев:

б.1) M делится на p и не делится на q;

б.2) M делится на q и не делится на p.

В связи с симметрией этих случаев, достаточно рассмотреть только один из них.

Будем предполагать, что имеет место случай б.1), т. е. $M = c \cdot p$ для некоторого $c \in N$ и $(M;q) = 1$. Тогда последовательно получаем:

$$M^{\varphi(q)} \equiv 1(\mathrm{mod}q), \qquad (2)$$

по теореме Эйлера (предложение 1 пункт 2));

$$(M^{\varphi(q)})^{\varphi(p)} \equiv 1(\mathrm{mod}\, q), \tag{3}$$

из сравнения (2) посредством возведения левой и правой частей этого сравнения в степень $\varphi(p)$ (предложение 1, пункт 1.в));

$$M^{\varphi(n)} \equiv 1(\mathrm{mod}\, q), \tag{4}$$

из сравнения (3) на основе мультипликативности функции Эйлера (предложение 1, пункт 3);

$$M^{\varphi(n)} \equiv 1 + kq, k \in N, \tag{5}$$

из сравнения (4) (предложение 1, пункт 1.г));

$$M^{\varphi(n)} \cdot c \cdot p \equiv c \cdot p + (kq) \cdot (cp), \tag{6}$$

из сравнения (5), посредством умножения левой и правой частей этого сравнения на $c \cdot p$ (предложение 1, пункт 1.б));

$$M^{\varphi(n)+1} \equiv M + (k \cdot c) \cdot n, \tag{7}$$

из сравнения (6), т.к. $c \cdot p = M$ и $n = p \cdot q$;

$$M^{\varphi(n)+1} \equiv M(\mathrm{mod} n), \tag{8}$$

из сравнения (7) (предложения 1, пункт 1.г)).

Предложение 3. Пусть $<\{n;e\};\{d;n\}>$ - криптосистемы с открытым ключом $\{n;e\}$. Тогда для любого неотрицательного числа M, меньшего n, из того, что $M^e \equiv C(\mathrm{mod} n)$ следует, что $C^d \equiv M(\mathrm{mod} n)$.

Доказательство. Из данного (по условию) сравнения $M^e \equiv C(\mathrm{mod} n)$, получаем, возводя его в степень d, сравнение

$$M^{ed} \equiv C^d(\mathrm{mod} n), \tag{9}$$

(предложение 1, пункт 1.б)).

Таким образом, для доказательства сравнения

$$C^d \equiv M(\mathrm{mod} n) \tag{10}$$

достаточно доказать, что

$$M^{ed} \equiv M(\mathrm{mod} n). \tag{11}$$

Действительно, если сравнение (11) будет доказано, то из этого сравнения и сравнения (9), используя свойства симметричности и транзитивности отношения сравнимости "$\equiv(\mathrm{mod} n)$" (предложение 1, пункт 1.а)) можно будет получить требуемое сравнение (10).

Переходя к доказательству сравнения (11), воспользуемся тем, что $e \cdot d \equiv 1(\mathrm{mod}\varphi(n))$, согласно выбора чисел e и d, как

составляющих открытого и закрытого ключей. Из сравнения $e \cdot d \equiv 1(\mathrm{mod}\,\varphi(n))$ получаем, что

$$e \cdot d \equiv l \cdot \varphi(n) + 1, \qquad 12)$$

для некоторого $l \in N$ (предложение 1, пункт 1.г)). Возводя теперь обе части сравнения (4) в степень l, будем иметь

$$M^{l \cdot \varphi(n)} \equiv 1(\mathrm{mod}\,q), \qquad 13)$$

(предложение 1, пункт 1.в)). Из сравнения (13) получаем, что

$$M^{l \cdot \varphi(n)} \equiv 1 + t \cdot q, \qquad (14)$$

для некоторого $t \in N$ (предложение 1, пункт 1.г)). Умножив обе части равенства (14) на число $c \cdot p$, получим:

$$M^{l \cdot \varphi(n)+1} = c \cdot p + (c \cdot p) \cdot (t \cdot q) = M + (c \cdot t) \cdot (p \cdot q) = M + (c \cdot t) \cdot n, \qquad (15)$$

(предложение 1 пункт 1.б)).

Т.к. $c \cdot p = M$ и $p \cdot q = n$. Из цепочки равенств (15), получаем, что

$$M^{l \cdot \varphi(n)+1} \equiv M(\mathrm{mod}\,n), \qquad 16)$$

(предложение 1, пункт 1.г)).

Из сравнения (16), с учетом равенства (12), получаем требуемое сравнение (10).

СПИСОК ЛИТЕРАТУРЫ

1 **Столлингс, В.** Криптография и защита сетей: принципы и практика, 2-е издание: пер. с англ. – М. : Издательский дом «Вильямс», 2001. – 672 с.

2 **Гончаров, С. С., Дроботун, Б. Н., Никитин, А. А.** Алгебраические и алгоритмические свойства логических исчислений. Монография. Часть I. – Новосибирск : Изд-во НГУ, 2008. – 221 с.

3 **Мусиралиева, Ш. Ж.** Прикладная криптография: Учебное пособие. – Алматы : Изд. ТОО «PrintS», 2004. – 73с.

4 **Виноградов, И. М.** Основы теории чисел. М. : Наука, 1972. – 167 с.

Павлодарский государственный университет
имени С. Торайгырова, Павлодар.
Материал поступил в редакцию 20.03.13.

Б. Н. Дроботун, Г. А. Сарсембаева

Ашық кілтпен берілген криптожүйелер (I)

С. Торайғыров атындағы Павлодар
мемлекеттік университеті, Павлодар қ.
Материал 20.03.13 редакцияға түсті.

B. N. Drobotun, G. A. Sarsembayeva

Public-key cryptosystems (I)

Pavlodar State University named after S. Toraigyrov, Pavlodar.
Material received on 20.03.13.

Берілген мақала ашық кілтпен шифрлеу технологияларына арналған жұмыстың бірінші бөлімі болып табылады. Бұл мақалада ашық кілтпен берілген криптожүйелерді құруда қолданылатын алгоритмдердің орынды дәлелдемесі және сипаттамасы келтіріледі.

This is the first part of the work dedicated to the technology of public key cryptography. This article provides a description and justification of evidentiary correctness algorithms used in the construction of public-key cryptosystems.

УДК 681.3.07

Б. Н. Дроботун, Г. А. Сарсембаева

КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ (II)

Предлагаемая статья является второй частью работы, посвященной технологиям шифрования с открытым ключом. В этой статье разрабатывается конкретная криптосистема, позволяющая кодировать (и декодировать) сообщения, записанные в алфавитах естественных языков.

1. Введение. Предлагаемая статья является второй частью работы, посвященной технологиям шифрования с открытым ключом.

В этой статье разрабатывается конкретная криптосистема, позволяющая кодировать (и декодировать) сообщения, записанные в алфавитах естественных языков.

Значительное внимание в работе уделяется построению и анализу примеров, посредством которых демонстрируются возможности построенной криптосистемы.

Роль примеров подобного содержания, сопровождающих процесс обучения естественно-математическим дисциплинам в период повсеместного внедрения коммуникационных и информационных технологий трудно переоценить.

Это связано с тем, что: «... как показывает история развития образовательных систем, отражающая историю развития общества, характеру примеров, задач и упражнений, аргументации и демонстрационному сопровождению процесса обучения в рамках любой специальности прикладного характера традиционно свойственно отражение специфики деятельности человека в ее массовом проявлении» [1, с. 20].

В настоящее время содержание и особенности этого демонстрационного сопровождения все еще определяют, в основном, идеи и представления, отражающие процессы механизации трудовой (то есть физической) деятельности человека. Тем не менее, с наступлением эры машинной математики, кибернетических устройств и робототехники, то есть эры повсеместного внедрения автоматических систем, в той или иной степени моделирующих мыслительную деятельность человека, подходы к разработке таких примеров, задач и упражнений, выбору аргументов и демонстраций должны постепенно меняться. Уже на языковом, ассоциативном уровне такое показательно-демонстрационное сопровождение должно вводить в мир образов и идей, обеспечивших приход эры информационных и коммуникационных технологий.

С этих позиций, приведенные в работе примеры наиболее показательным образом вводят в область приложений алгебры и дискретной математики.

2. Примеры применения. Продемонстрируем технологию применения криптосистемы $<\{n;e\};\{d;n\}>$ на конкретном примере.

В качестве простых чисел p и q выбираем, соответственно, числа 3 и 11. Тогда $n = p \cdot q = 3 \cdot 11 = 33$. Понятно, что число $n = 33$ не только теоретически, но и практически можно легко разложить на два простых множителя. Т. е. криптосистема предлагаемого примера может быть рассекречена, при необходимости, без особого труда. Но, в данном случае, значимость примера определяется не надежностью, предложенного в нем шифра, а демонстрационными задачами, решение которых заведомо предлагает единство относительной простоты и доступности для восприятия с детальным воспроизведением всех технологических процессов.

Здесь уместно вспомнить классический пример о беседе двух математиков, когда один из них пытался пояснить суть своих результатов другому, используя сложнейшие построения в n-мерном пространстве и трудно воспринимаемую систему символических обозначений. Второй же математик, остановив его, попросил рассказать, как все это выглядит в случае $n = 2$.

В предложенном примере $\varphi(n) = \varphi(3 \cdot 11) = \varphi(3) \cdot \varphi(11) = 2 \cdot 10 = 20$ и в качестве параметра e можно взять число 13. Решая, далее, сравнение $ed \equiv 1 (\mathrm{mod}\, n)$, которое, в рассматриваемом случае, примет вид $13d \equiv 1 (\mathrm{mod}\, 20)$, находим параметр $d = 17$. Таким образом, мы построили криптосистему $< \{33;13\}; \{17;33\} >$ с открытым ключом $\{33;13\}$.

Пусть, к примеру передаче подлежит сообщение

$$X = < 11100101010010 >.$$

Находя из неравенства $2^k \le 33 < 2^{k+1}$ вида (1) длину блока в разбиении последовательности X, получаем, что $k = 5$. Разбивая эту последовательность справа - налево на блоки длины 5, будем иметь

$$\underset{1-ый\ \ блок}{\underline{1110}} \qquad \underset{2-ой\ \ блок}{\underline{01010}} \qquad \underset{3-ий\ \ блок}{\underline{10010}} \tag{1}$$

Т.к. первый блок в разбиении (1) имеет длину 4, то дополняем его до блока длины 5, приписывая один 0 слева. По полученным блокам

$$\sigma_1 = < 01110 >;\ \sigma_2 = < 01010 >;\ \sigma_3 = < 10010 >,$$

находим, соответственно, натуральные числа $M_1 = 14$; $M_2 = 10$ и $M_3 = 18$, двоичными разложениями которых эти блоки являются. Используя соотношение $C_i \equiv M_i^e (\mathrm{mod}\, n)$ $i = 1,2,3$, шифруем числа

$M_1;M_2;M_3$, соответственно числами $C_1 \equiv 14^{13}(\mathrm{mod}33)$; $C_2 \equiv 10^{13}(\mathrm{mod}33)$; $C_3 \equiv 18^{13}(\mathrm{mod}33)$.

Напомним, что $C_1;C_2;C_3$ выбираются, как наименьшие неотрицательные вычеты по модулю $n=33$ чисел $14^{13};10^{13};18^{13}$, соответственно.

Отсюда:

$C_1 \equiv 14^{13} = (14^2)^6 \cdot 14 \equiv 31^6 \cdot 14 \equiv (31^2)^3 \cdot 14 \equiv 4^3 \cdot 14 \equiv 896 \equiv 5(\mathrm{mod}33)$;

$C_2 \equiv 10^{13} = (10^2)^6 \cdot 10 \equiv 1^6 \cdot 10 \equiv 10(\mathrm{mod}33)$;

$C_3 \equiv 18^{13} \equiv (18^2)^6 \cdot 18 \equiv 27^6 \cdot 18 \equiv (27^2)^3 \cdot 18 \equiv 3^3 \cdot 18 \equiv 486 \equiv 24(\mathrm{mod}33)$.

Записями найденных чисел $C_1=5;C_2=10;C_3=24$ в двоичной системы счисления будут новые двоичные блоки:

$$\underset{C_1}{\overline{00101}} \quad \underset{C_2}{\overline{01010}} \quad \underset{C_3}{\overline{11000}}$$

Формируя из этих блоков единую двоичную последовательность, получаем шифрованное сообщение

$$X' = <0010101010\,11000>,$$

которое и будет отправлено.

Адресат, получив это сообщение, по личному коду $\{17;33\}$ находит из соотношения (1) длину блока $k=5$, разбивает (справа - налево) двоичную последовательность X' на блоки этой длины и по полученным блокам восстанавливает десятичные представления этих двоичных блоков, т. е. числа $C_1=5$; $C_2=10$; $C_3=24$. При «расшифровке» найденных чисел по формуле $M_i \equiv C_i^{17}(\mathrm{mod}33)$ $(i=1,2,3)$, адресат должен будет найти наименьшие неотрицательные вычеты чисел $5^{17};10^{17};24^{17}$ по модулю 33.

Согласно теоретическим концептам, заложенным в основу построения криптосистемы с открытым ключом, эти вычеты должны быть равны, соответственно, $14=M_1;10=M_2;18=M_3$. Действительно, проводя необходимые вычисления, получаем:

$5^{17} = (5^3)^5 \cdot 5^2 \equiv (125)^5 \cdot 25 \equiv (26^2)^2 \cdot 26 \cdot 25 \equiv 16^2 \cdot 24 \equiv 25 \cdot 23 \equiv 14(\mathrm{mod}33)$;

$10^{17} = (10^3)^5 \cdot 10^2 \equiv (1000)^5 \cdot 100 \equiv 10 \cdot 1 \equiv 10(\mathrm{mod}33)$;

$24^{17} = (24^2)^8 \cdot 24 \equiv (15^2)^4 \cdot 24 \equiv (27^2)^2 \cdot 24 \equiv 9 \cdot 24 \equiv 216 \equiv 18(\mathrm{mod}33)$.

Переводя, далее числа 14; 10; 18 в двоичную систему счисления, адресат получает двоичные блоки $<01110>;<01010>;<10010>$. Формируя из этих блоков единую двоичную последовательность, он формирует расшифрованный «текст»

$$X = <0111001010\,10010>$$

переданного (зашифрованного) сообщения.

3. Криптосистемы с открытым ключом для работы с сообщениями в алфавитах естественных языков. В заключительной части работы предпринимается опыт построения криптосистемы с открытым ключом, применяя которую можно будет кодировать (и, соответственно, декодировать) сообщения, заданные в алфавите казахского языка и в алфавитах других естественных языков. Т.к. алфавит этого языка содержит 42 буквы, то, с учетом необходимости кодирования (кроме букв) еще и некоторых вспомогательных символов (таких, как «,» - запятая, «:» - двоеточие, «!» - восклицательный знак и т.п.), параметр n строящийся криптосистемы должен удовлетворять условию $n > 52$. Если в качестве простых чисел p и q взять, соответственно, числа 5 и 13, то полученное число $n = p \cdot q = 5 \cdot 13 = 65$ будет удовлетворять вышеприведенному условию.

Т.к. $\varphi(n) = \varphi(65) = \varphi(5 \cdot 13) = 4 \cdot 12 = 48$, то в качестве параметра e можно выбрать число 11. Решая сравнение $11d \equiv 1 (\mathrm{mod}\, 48)$, находим $d = 35$. Вычислив все параметры, получаем криптосистему $<\{65;11\};\{35;65\}>$ с открытым ключом $\{65;11\}$.

Отождествим теперь буквы алфавита казахского языка с порядковыми номерами их следования в этом алфавите. Т.к. $n = 65$, то, находя натуральное число k из условия $2^k \le 65 < 2^{k+1}$, получаем, что $k = 6$. Таким образом, номер каждой буквы алфавита казахского языка можно записать в виде двоичной последовательности длины 6. В предлагаемой далее таблице (смотри таблицу 1) даны буквы этого алфавита, указаны их порядковые номера и двоичные разложения этих номеров, как чисел, заданных в десятичной системе счисления.

Таблица 1 – Двоичное представление букв и вспомогательных символов алфавита казахского языка

А	1	000001	К	14	001110	Ұ	27	011011	Э	40	101000
Ә	2	000010	Қ	15	001111	Ү	28	011100	Ю	41	101001
Б	3	000011	Л	16	010000	Ф	29	011101	Я	42	101010
В	4	000100	М	17	010001	Х	30	011110	,	43	101011
Г	5	000101	Н	18	010010	Һ	31	011111	!	44	101100
Ғ	6	000110	Ң	19	010011	Ц	32	100000	:	45	101101
Д	7	000111	О	20	010100	Ч	33	100001	-	46	101110
Е	8	001000	Ө	21	010101	Ш	34	100010	?	47	101111
Ё	9	001001	П	22	010110	Щ	35	100011	(	48	110000
Ж	10	001010	Р	23	010111	Ъ	36	100100	)	49	110001
З	11	001011	С	24	011000	Ы	37	100101	;	50	110010
И	12	001100	Т	25	011001	І	38	100110	«	51	110011
Й	13	001101	У	26	011010	Ь	39	100111	»	52	110100

Пусть требуется передать сообщение: АСТАНА, предварительно зашифровав его средствами построенной криптосистемы. Сведем все необходимые для этого данные в единую таблицу (смотри таблицу 2). В 1-ой строке этой таблицы указаны буквы передаваемого сообщения в порядке их следования в этом сообщении, во 2-ой строке – обозначения $M_i (i = 1,2,3,4,5,6)$ порядковых номеров этих букв в алфавите казахского языка, в 3-ей строке – их порядковые номера, в 4-ой строке – двоичные разложения этих номеров.

Таблица 2 – Двоичное представление сообщения «АСТАНА»

А	С	Т	А	Н	А
M_1	M_2	M_3	M_4	M_5	M_6
1	24	25	1	18	1
000001	011000	011001	000001	010010	000001

Таким образом, передаче подлежит сообщение

$$X = < 000001011000011001000001010010000001 >,$$

являющееся двоичной версией исходного сообщения: АСТАНА.

Шифруя числа $M_1 = 1; M_2 = 24; M_3 = 25; M_4 = 1; M_5 = 18; M_6 = 1$, на основе соотношения $C_i \equiv M_i^e (\mathrm{mod}\, 65)$, получаем:

$C_1 \equiv 1^{11} \equiv 1(\mathrm{mod}65)$

$C_2 \equiv (24^2)^5 \cdot 24 \equiv (56^2)^2 \cdot 56 \cdot 24 \equiv 16^2 \cdot 56 \cdot 24 \equiv 19(\mathrm{mod}65)$

$C_3 \equiv 25^{11} = (25^2)^5 \cdot 25 \equiv (40^2)^2 \cdot 40 \cdot 25 \equiv 40^2 \cdot 40 \cdot 25 \equiv 25(\mathrm{mod}65)$

$C_4 \equiv 1^{11} \equiv 1(\mathrm{mod}65);$

$C_5 \equiv 18^{11} = (18^2)^5 \cdot 18 \equiv (64^2)^2 \cdot 64 \cdot 18 \equiv 1 \cdot 64 \cdot 18 \equiv 47 \equiv 25(\mathrm{mod}65);$

$C_6 \equiv 1^{11} \equiv 1(\mathrm{mod}65).$

Записывая найденные наименьшие неотрицательные вычеты $C_1 = 1; C_2 = 19; C_3 = 25; C_4 = 1; C_5 = 47; C_6 = 1$ в двоичной системе счисления, получим следующие блоки длины 6:

$$\underset{\text{блок } C_1}{\underline{000001}} \quad \underset{\text{блок } C_2}{\underline{010011}} \quad \underset{\text{блок } C_3}{\underline{011001}} \quad \underset{\text{блок } C_4}{\underline{000001}} \quad \underset{\text{блок } C_5}{\underline{101111}} \quad \underset{\text{блок } C_6}{\underline{000001}}$$

Таким образом, готовый к отправке зашифрованный вариант X' исходного сообщения X будет иметь вид:

$$X' = <000001010011011001000001101111000001>$$

Как и в примере из пятого параграфа, адресат, получив сообщение X', по значению параметра $n = 65$ из своего личного кода находит длину блока, на которые нужно будет разбить это сообщение.

При этом, он использует неравенство

$$2^k \le 65 < 2^{k+1}.$$

Получив из этого неравенства значение $k = 6$, он разбивает сообщение X' (справа - налево) на блоки длины 6:

$$\underset{1-й\ блок}{\underline{000001}} \quad \underset{2-ой\ блок}{\underline{010011}} \quad \underset{3-ий\ блок}{\underline{011001}} \quad \underset{4-ый\ блок}{\underline{000001}} \quad \underset{5-ый\ блок}{\underline{101111}} \quad \underset{6-ой\ блок}{\underline{000001}}.$$

Восстановив по полученным двоичным блокам числа

$$C_1 = 1; \quad C_2 = 19; \quad C_3 = 25; \quad C_4 = 1; \quad C_5 = 47; \quad C_6 = 1,$$

адресат находит соответствующие им номера $M_1; M_2; M_3; M_4; M_5; M_6$ букв алфавита, используя соотношение $M_i = C_i^d (\mathrm{mod}\, n)$, при $d = 35$, $n = 65$, $i = 1;2;3;4;5;6$:

$M_1 = 1^{35} \equiv 1(\mathrm{mod}35)$;

$M_2 = 19^{35} = (19^2)^{17} \cdot 19 \equiv (36^2)^8 \cdot 36 \cdot 19 \equiv (61^2)^4 \cdot 36 \cdot 19 \equiv (16^2)^2 \cdot 36 \cdot 19 \equiv$
$\equiv 61^2 \cdot 36 \cdot 19 \equiv 16 \cdot 36 \cdot 19 \equiv 24(\mathrm{mod}65)$;

$M_3 = 25^{35} = (25^2)^{17} \cdot 25 \equiv (40^2)^8 \cdot 40 \cdot 25 \equiv (40^2)^4 \cdot 40 \cdot 25 \equiv (40^2)^2 \cdot 40 \cdot 25 \equiv$
$\equiv 40^2 \cdot 40 \cdot 25 \equiv 25(\mathrm{mod}65)$;

$M_4 = 1^{35} \equiv 1(\mathrm{mod}35)$;

$M_5 = 47^{35} = (47^2)^{17} \cdot 47 \equiv (64^2)^8 \cdot 64 \cdot 47 \equiv 1^8 \cdot 64 \cdot 47 \equiv 18(\mathrm{mod}65)$;

$M_6 = 1^{35} \equiv 1(\mathrm{mod}35)$.

По найденным порядковым номерам

$M_1 = 1; M_2 = 24; M_3 = 25; M_4 = 1; M_5 = 18; M_6 = 1$

букв А; С; Т; А; Н; А он получает дешифрованное сообщение АСТАНА.

Пусть теперь требуется передать сообщение:

«АЛҒА, ҚАЗАҚСТАН!»

Вновь сведем все данные в единую таблицу (смотри таблицу 3)

Таблица 3 – Двоичное представление сообщения «АЛҒА, ҚАЗАҚСТАН!»

А	Л	Ғ	А	,	Қ	А	З	А	Қ	С	Т	А	Н	!
M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}
1	16	6	1	43	15	1	11	1	15	24	25	1	18	44
00	01	00	00	10	00	00	00	00	00	01	01	00	01	10
00	00	01	00	10	11	00	10	00	11	10	10	00	00	11
01	00	10	01	11	11	01	11	01	11	00	01	01	10	00

Таким образом, передаче подлежит сообщение

X = <000001010000000110000001101011001111000001
0010110000010011111011000011001000001010010101100>

Шифруя числа

$M_1 = 1; M_2 = 16; M_3 = 6; M_4 = 1; M_5 = 43; M_6 = 15; M_7 = 1; M_8 = 11;$
$M_9 = 1; M_{10} = 15; M_{11} = 24; M_{12} = 25; M_{13} = 1; M_{14} = 18; M_{15} = 44,$

на основе соотношения $C_i \equiv M_i^e(\mathrm{mod}65)$, получаем:

$C_1 \equiv 1^{11} = 1(\mathrm{mod}65);$

$C_2 \equiv 16^{11} = (16^2)^5 \cdot 16 \equiv (61^2)^2 \cdot 61 \cdot 16 \equiv 61 \cdot 61 \cdot 16 \equiv 61(\mathrm{mod}65)$

$C_3 \equiv 6^{11} = (6^2)^5 \cdot 6 \equiv (36^2)^2 \cdot 36 \cdot 6 \equiv 61^2 \cdot 36 \cdot 6 \equiv 16 \cdot 36 \cdot 6 \equiv 11(\mathrm{mod}65)$

$C_4 \equiv 1^{11} = 1(\mathrm{mod}65)$

$C_5 \equiv 43^{11} = (43^2)^5 \cdot 43 \equiv (29^2)^2 \cdot 29 \cdot 43 \equiv 16 \cdot 29 \cdot 43 \equiv 62(\mathrm{mod}65)$

$C_6 \equiv 15^{11} = (15^2)^5 \cdot 15 \equiv (30^2)^2 \cdot 30 \cdot 15 \equiv 35 \cdot 30 \cdot 15 \equiv 20(\mathrm{mod}65)$

$C_7 \equiv 1^{11} = 1(\mathrm{mod}65)$

$C_8 \equiv 11^{11} = (11^2)^5 \cdot 11 \equiv (56^2)^2 \cdot 56 \cdot 11 \equiv 61 \cdot 56 \cdot 11 \equiv 6(\mathrm{mod}65)$

$C_9 \equiv 1^{11} = 1(\mathrm{mod}65)$

$C_{10} \equiv 15^{11} = (15^2)^5 \cdot 15 \equiv (30^2)^2 \cdot 30 \cdot 15 \equiv 35 \cdot 30 \cdot 15 \equiv 20(\mathrm{mod}65)$

$C_{11} \equiv 24^{11} = (24^2)^5 \cdot 24 \equiv (56^2)^2 \cdot 56 \cdot 24 \equiv 61 \cdot 56 \cdot 24 \equiv 19(\mathrm{mod}65)$

$C_{12} \equiv 25^{11} = (25^2)^5 \cdot 25 \equiv (40^2)^2 \cdot 40 \cdot 25 \equiv 40 \cdot 40 \cdot 25 \equiv 25(\mathrm{mod}65)$

$C_{13} \equiv 1^{11} = 1(\mathrm{mod}65)$

$C_{14} \equiv 18^{11} = (18^2)^5 \cdot 18 \equiv (64^2)^2 \cdot 64 \cdot 18 \equiv 1^2 \cdot 64 \cdot 18 \equiv 47(\mathrm{mod}65)$

$C_{15} \equiv 44^{11} = (44^2)^5 \cdot 44 \equiv (51^2)^2 \cdot 51 \cdot 44 \equiv 1^2 \cdot 51 \cdot 44 \equiv 34(\mathrm{mod}65).$

Записывая найденные наименьшие неотрицательные вычеты $C_1 = 1; C_2 = 61; C_3 = 11; C_4 = 1; C_5 = 62; C_6 = 20; C_7 = 1; C_8 = 6; C_9 = 1; C_{10} = 20;$ $C_{11} = 19; C_{12} = 25; C_{13} = 1; C_{14} = 47; C_{15} = 34$

в двоичной системе счисления, получим следующие блоки длины 6:

$$\underbrace{000001}_{C_1}\ \underbrace{111101}_{C_2}\ \underbrace{001011}_{C_3}\ \underbrace{000001}_{C_4}\ \underbrace{111110}_{C_5}\ \underbrace{010100}_{C_6}\ \underbrace{000001}_{C_7}\ \underbrace{001000}_{C_8}$$

$$\underbrace{000001}_{C_9}\ \underbrace{010100}_{C_{10}}\ \underbrace{010011}_{C_{11}}\ \underbrace{011001}_{C_{12}}\ \underbrace{000001}_{C_{13}}\ \underbrace{101111}_{C_{14}}\ \underbrace{100010}_{C_{15}}$$

Таким образом, готовый к отправке зашифрованный вариант X' исходного сообщения X будет иметь вид:

$X' =$ < 000001111101 001011000001111110 010100 000001001000000001 010100 010011011001000001101111100010>

Получив это сообщение, адресат действует по той же схеме, что была продемонстрирована в предыдущем примере. Приводимые далее вычисления показывают, что при декодировании сообщения X' адресат действительно получит порядковые номера букв исходного сообщения:

«АЛҒА, ҚАЗАҚСТАН!»

$1^{35} = 1(\mathrm{mod}35)$;

$61^{35} = (61^2)^{17} \cdot 61 \equiv (16^2)^8 \cdot 16 \cdot 61 \equiv (61^2)^4 \cdot 16 \cdot 61 \equiv (16^2)^2 \cdot 16 \cdot 61 \equiv$
$\equiv 61^2 \cdot 16 \cdot 61 \equiv 16 \cdot 16 \cdot 61 \equiv 16(\mathrm{mod}35)$;

$11^{35} = (11^2)^{17} \cdot 11 \equiv (56^2)^8 \cdot 56 \cdot 11 \equiv (16^2)^4 \cdot 56 \cdot 11 \equiv (61^2)^2 \cdot 56 \cdot 11 \equiv 16^2 \cdot 56 \cdot 11 \equiv$
$\equiv 61 \cdot 56 \cdot 11 \equiv 6(\mathrm{mod}35)$;

$1^{35} = 1(\mathrm{mod}35)$;

$62^{35} = (62^2)^{17} \cdot 62 \equiv (9^2)^8 \cdot 9 \cdot 62 \equiv (16^2)^4 \cdot 9 \cdot 62 \equiv (61^2)^2 \cdot 9 \cdot 62 \equiv 16^2 \cdot 9 \cdot 62 \equiv$
$\equiv 61 \cdot 9 \cdot 62 \equiv 43(\mathrm{mod}35)$;

$20^{35} = (20^2)^{17} \cdot 20 \equiv (10^2)^8 \cdot 10 \cdot 20 \equiv (35^2)^4 \cdot 10 \cdot 20 \equiv (55^2)^2 \cdot 10 \cdot 20 \equiv 35^2 \cdot 10 \cdot 20 \equiv$
$\equiv 55 \cdot 10 \cdot 20 \equiv 15(\mathrm{mod}35)$;

$1^{35} = 1(\mathrm{mod}35)$;

$6^{35} = (6^2)^{17} \cdot 6 \equiv (36^2)^8 \cdot 36 \cdot 6 \equiv (61^2)^4 \cdot 36 \cdot 6 \equiv (16^2)^2 \cdot 36 \cdot 6 \equiv 61^2 \cdot 36 \cdot 6 \equiv$
$\equiv 16 \cdot 36 \cdot 6 \equiv 11(\mathrm{mod}35)$;

$1^{35} = 1(\mathrm{mod}35)$;

$20^{35} = (20^2)^{17} \cdot 20 \equiv (10^2)^8 \cdot 10 \cdot 20 \equiv (35^2)^4 \cdot 10 \cdot 20 \equiv (55^2)^2 \cdot 10 \cdot 20 \equiv$
$\equiv 35^2 \cdot 10 \cdot 20 \equiv 55 \cdot 10 \cdot 20 \equiv 15(\mathrm{mod}35)$;

$19^{35} = (19^2)^{17} \cdot 19 \equiv (36^2)^8 \cdot 36 \cdot 19 \equiv (61^2)^4 \cdot 36 \cdot 19 \equiv (16^2)^2 \cdot 36 \cdot 19 \equiv$
$\equiv 61^2 \cdot 36 \cdot 19 \equiv 16 \cdot 36 \cdot 19 \equiv 24(\mathrm{mod}35)$;

$25^{35} = (25^2)^{17} \cdot 25 \equiv (40^2)^8 \cdot 40 \cdot 25 \equiv (40^2)^4 \cdot 40 \cdot 25 \equiv (40^2)^2 \cdot 40 \cdot 25 \equiv$
$\equiv 40^2 \cdot 40 \cdot 25 \equiv 40 \cdot 40 \cdot 25 \equiv 25(\mathrm{mod}35)$;

$1^{35} = 1(\mathrm{mod}35)$;

$47^{35} = (47^2)^{17} \cdot 47 \equiv (64^2)^8 \cdot 64 \cdot 47 \equiv 1^8 \cdot 64 \cdot 47 \equiv 18(\mathrm{mod}\,35)$;

$34^{35} = (34^2)^{17} \cdot 34 \equiv (51^2)^8 \cdot 51 \cdot 34 \equiv 1^8 \cdot 51 \cdot 34 \equiv 44(\mathrm{mod}\,35)$.

Аналогичным образом, отождествляя буквы алфавита русского языка с порядковыми номерами их следования в этом алфавите, построим криптограмму с открытым ключом для шифрования сообщений, записанных на русском языке. Т.к. алфавит русского языка содержит 33 буквы, то, с учетом необходимости шифрования символов пунктуационного назначения, параметр n криптосистемы

должен удовлетворять условию $n \geq 33$. Из неравенства $2^k \leq 33 < 2^{k+1}$ находим, что $k = 6$, т. е. для того, чтобы зашифровать все буквы русского алфавита и некоторые дополнительные символы, нужно использовать блоки длины 6, как и при шифровании сообщений в алфавите казахского языка.

Таким образом, построенная ранее криптосистема $\langle\{65;11\},\{35;65\}\rangle$, может быть применена и при шифровании сообщений в алфавите русского языка.

В этом случае, исходная таблица будет иметь следующий вид: (смотри таблицу 4).

Таблица 4 – Двоичное представление букв и вспомогательных символов алфавита казахского языка.

А	1	000001	Л	13	001101	Ч	25	011001
Б	2	000010	М	14	001110	Ш	26	011010
В	3	000011	Н	15	001111	Щ	27	011011
Г	4	000100	О	16	010000	Ъ	28	011100
Д	5	000101	П	17	010001	Ы	29	011101
Е	6	000110	Р	18	010010	Ь	30	011110
Ё	7	000111	С	19	010011	Э	31	011111
Ж	8	001000	Т	20	010100	Ю	32	100000
З	9	001001	У	21	010101	Я	33	100001
И	10	001010	Ф	22	010110	,	34	100010
Й	11	001011	Х	23	010111	:	35	100011
К	12	001100	Ц	24	011000	-	36	100100

СПИСОК ЛИТЕРАТУРЫ

1. **Гончаров, С. С., Дроботун, Б. Н., Никитин, А. А.** О логико-алгебраической составляющей математического образования (I). // Вестник ЕНУ им. Гумилева : Астана, 2012. – № 4. – С. 15-22.

Павлодарский государственный университет
имени С. Торайгырова, Павлодар.
Материал поступил в редакцию 20.03.13.

Б. Н. Дроботун, Г. А. Сарсембаева

Ашық кілтпен берілген криптожүйелер (II)

С. Торайғыров атындағы
Павлодар мемлекеттік университеті, Павлодар қ.
Материал 20.03.13 редакцияға түсті.

B. N. Drobotun, G. A. Sarsembayeva

Public-key cryptosystems (II)

Pavlodar State University named after S. Toraigyrov, Pavlodar.
Material received on 20.03.13.

Берілген мақала ашық кілтпен шифрлеу технологияларына арналған жұмыстың екінші бөлімі болып табылады. Бұл мақалада жаратылыстану тілдері әліпбиінде жазылған хабарламаларды кодтауға (және қайта кодтауға) мүмкіндік беретін нақты криптожүйе құрастырылады.

The present article is the second part of technology in public key cryptography. In this paper, we develop a specific cryptosystem to encode (and decode) messages written in alphabets of natural languages.

УДК 533.6.011

А. Т. Дыйканова

СТАЦИОНАРНАЯ ЗАДАЧА ОКОЛОЗВУКОВОГО ТЕЧЕНИЯ СЖИМАЕМОЙ ЖИДКОСТИ В СОПЛАХ

В работе рассмотрена и исследована пространственная стационарная задача безвихревого течения газа в соплах

В работе исследуется пространственное потенциальное стационарное течение идеального газа, подчиненный адиабатическому закону. Основные закономерности движения сжимаемой жидкости таковы: уравнение неразрывности имеет вид [2]

$$\frac{\partial \rho}{\partial t} + \operatorname{div}\rho\bar{v} = 0, \qquad (1)$$

а уравнение Эйлера как

$$\frac{\partial \rho}{\partial t} + \operatorname{grad}\frac{v^2}{2} - \bar{v}\cdot r_0 t\bar{v} = -\frac{1}{\rho}\operatorname{grad}\rho. \qquad (2)$$

Уравнение, выражающее факт сохранения удельной энтропии S в частице газа будет [1,2]

$$\frac{\partial S}{\partial t} + \bar{v}\operatorname{grad}S = 0. \qquad (3)$$

Предполагается так же, диссипативных процессов в среде не происходят т. е. считаем среду лишенной вязкости и теплопроводности. И наконец, к уравнениям (1-3) необходимо присоединить уравнение состояния среды

$$P = P(\rho, s), \qquad 4)$$

которое связывает давление с плотностью и удельной энтропией, явный вид устанавливается из термодинамических соображений или экспериментальными методами. Таким образом, уравнения (1-4) образуют замкнутую систему.

Прежде чем приступить к строгому изложению математической теории сопла Лаваля, отметим, отсутствие скачков уплотнения является одним из основных требований, предъявляемых к потоку через сопло Лаваля. Поэтому в дальнейшем будут рассматриваться только безударные течения. В таких течениях энтропия остается одинаковой во всем пространстве и не меняется со временем всюду вдоль потока. Далее потребуем, чтобы поток на входе в сопло был безвихревым, т. е. циркуляция скорости потока обращается в нуль по любому замкнутому контуру, движущимся вместе с частицами. Это означает что существует такая скалярная функция для которой справедлива

$$\bar{v} = \operatorname{grad}\varphi \qquad (5)$$

называемой потенциалом скорости. Если $u = \varphi_x$, $v = \varphi_y$, $\omega = \varphi_z$ - составляющие вектора скорости соответственно, вдоль осей x,y,z декартовой системы координат, то с учетом вышесказанного, уравнение неразрывности запишется в виде [3]

$$(a^2 - \varphi_x^2)\varphi_{xx} + (a^2 - \varphi_y^2)\varphi_{yy} + (a^2 - \varphi_z^2)\varphi_{zz} - 2(\varphi_x\varphi_y\varphi_{xy} + \varphi_x\varphi_z\varphi_{xz} + \varphi_y\varphi_z\varphi_{yz}) - \\ - 2(\varphi_x\varphi_{xt} + \varphi_y\varphi_{yt} + \varphi_z\varphi_{zt}) - \varphi_{tt} = 0 \qquad (6)$$

В полученном выражении, скорость звука a должна быть выражена через производные потенциала скорости при помощи

равенства $a^2 = (\frac{\partial P}{\partial \rho})_S$ и интеграла Лагранжа – Коши (где W - удельная энтальния).

$$\frac{\partial \varphi}{\partial t} + \frac{v^2}{2} = W - const \qquad (7)$$

Наличия интеграла Лагранжа – Коши позволяет свести задачи об изэнтропичесих безвихревых течениях газа к изучению одного дифференциального уравнения второго порядка в частных производных. В этом заключается относительная простота их математического исследования.

Уравнение (6) для стационарных течений можно записать так:

$$a^2(\varphi_{xx} + \varphi_{yy} + \varphi_{zz}) = \varphi_x(v^2)_x + \varphi_y(v^2)_y + \varphi_z(v^2)_z, \qquad (8)$$

где $$v^2 = (\varphi_x)^2 + (\varphi_y)^2 + (\varphi_z)^2 \qquad (9)$$

или из уравнения (6). имеем [3]

$$(a^2 - \varphi_x^2)\varphi_{xx} + (a^2 - \varphi_y^2)\varphi_{yy} + (a^2 - \varphi_z^2)\varphi_{zz} - \\ -2[\varphi_x\varphi_y\varphi_{xy} + \varphi_x\varphi_z\varphi_{xz} + \varphi_y\varphi_z\varphi_{yz}] = 0 \qquad (10)$$

a - скорость звука, имеющая вид:

$$a^2 = \frac{\gamma+1}{2}a_*^2 - \frac{\gamma-1}{2}(\varphi_x^2 + \varphi_y^2 + \varphi_z^2) \qquad (11)$$

$\gamma = c_p/c_v$, c_p, c_v - удельные теплоемкости газа при постоянном давлении и постоянном объеме, соответственно.

a_* - критическая скорость звука.

В работе ищется решение для потенциала скорости $\varphi(x, y, z)$, соответствующее непрерывному околозвуковому пространственному течению в канале (сопло), с начальными данными на оси симметрии

$$\varphi(x,0,0) = d_1x + d_2x^2 + d_3x^3 + \ldots, \quad \varphi_x(x,0,0) = 0, \quad \varphi_y(x,0,0) = 0 \qquad (12)$$

Вначале подставим (11) в (10) и после некоторых преобразований имеем (где $h^2 = (\gamma-1)/(\gamma+1)$)

$$[a_*^2 - \varphi_x^2 - h^2(\varphi_x^2 + \varphi_y^2)]\varphi_{xx} + [a_*^2 - \varphi_x^2 - h^2(\varphi_x^2 + \varphi_y^2)]\varphi_{yy} + \\ + [a_*^2 - \varphi_y^2 - h^2(\varphi_x + \varphi_y)]\varphi_{zz} - \frac{4}{\gamma+1}[\varphi_x\varphi_y\varphi_{xy} + \varphi_x\varphi_z\varphi_{xz} + \varphi_y\varphi_z\varphi_{yz}] = 0 \qquad (13)$$

Нахождение решений квазилинейного уравнения в частных производных второго порядка (13) представляет большую трудность, так как рассматриваемое уравнение нелинейно. Поэтому

перейдем к выводу приближенных уравнений описывающих течения в околозвуковом диапозоне скоростей. Вопросами линеаризации полного уравнения для потенциала скоростей посвящены ряд работ, где одним из наиболее широко употребляемых методов упрощения газовой динамики является метод малых возмущений или метод малого параметра. Рассмотрим течение идеального газа со скоростями, незначительно отличающимися от критической скорости в начале, которое имеет две плоскости симметрии. Прямую, по которой пересекаются эти плоскости, будем считать осью сопла и предположим, что она совпадает с осью абсцисс.

Решение уравнения (13) будем искать в виде ряда

$$\varphi(x, y, z) = a_*(x + \varepsilon\varphi_0 + \varepsilon^2\varphi_1 + \varepsilon^3\varphi_2 + \ldots), \qquad (14)$$

где ε - малый параметр и он равен

$$\varepsilon = 1 - M_\infty^2$$

где M_∞^2 - число Маха бесконечности вверх по потоку.

С учетом (14), а так же $\bar{y} = \sqrt{\gamma+1}\,y$, $\bar{z} = \sqrt{\gamma+1}\,z$, получим первые три приближения уравнения $-\varphi_{0x}\varphi_{0xx} + \varphi_{0yy} + \varphi_{0zz} = 0$ (15)

$$-\varphi_{0x}\varphi_{1xx} + \varphi_{1yy} + \varphi_{1zz} - \varphi_{0xx}\varphi_{1x} =$$

$$= \frac{1}{\gamma-1}\left\{\varphi_{0x}\left[\frac{1}{2}\varphi_{0x}\varphi_{0xx} + (\gamma-1)(\varphi_{0yy} + \varphi_{0zz})\right] + 2(\varphi_{0y}\varphi_{0xy} + \varphi_{0z}\varphi_{0xz})\right\} \qquad (15а)$$

$$-\varphi_{0x}\varphi_{2xx} + \varphi_{2yy} + \varphi_{2zz} - \varphi_{0xx}\varphi_{2x} =$$

$$= \frac{1}{\gamma-1}\left\{\varphi_{0x}\left[\frac{1}{2}\varphi_{0x}\varphi_{1xx} + \frac{1}{\gamma-1}\varphi_{1x}\varphi_{1xx}\right] + \frac{\gamma-1}{2(\gamma+1)}\varphi_{0xx}(\varphi_{0y}^2 + \varphi_{0z}^2) + \right.$$

$$+ \frac{\gamma-1}{2(\gamma+1)}\varphi_{0x}(\varphi_{0yy} + \varphi_{0zz}) + (\gamma-1)\varphi_{0x}(\varphi_{1yy} + \varphi_{1zz}) + (\gamma-1)\varphi_{1x}(\varphi_{0yy} + \varphi_{0zz}) +$$

$$+ (\gamma+1)\varphi_{1x}\varphi_{1xx} + \frac{2}{\gamma-1}\varphi_{0x}(\varphi_{0y}\varphi_{0xy} + \varphi_{0z}\varphi_{0xz}) + 2(\varphi_{0xy}\varphi_{1y} + \varphi_{0y}\varphi_{1xy} +$$

$$\left. + \varphi_{0xz}\varphi_{1z} + \varphi_{0z}\varphi_{1xz})\right\} \qquad (15а)$$

- -

$$-\varphi_{0x}\varphi_{nxx} + \varphi_{nyy} + \varphi_{nzz} - \varphi_{0xx}\varphi_{nx} = F(\varphi_0, \varphi_1, \ldots, \varphi_{n-2}, \varphi_{n-1}) \qquad (15в)$$

Уравнения (15-15в) являются рекуррентной системой дифференциальных уравнений для исследования установившихся потенциальных течений газа в трансзвуковом режиме скоростей.

Уравнение (15) называется уравнением Кармана, оно является фундаментальным при изучении течений газа с околозвуковыми скоростями. Оно также нелинейно и принцип суперпозиции решений для него несправедлив и тем не менее оно значительно проще полного уравнения для потенциала скорости (13). Чтобы установить основные свойства потока вблизи горловины сопла необходимо подробно рассмотреть некоторые частные решения уравнения (15), причем немаловажную роль играют также автомодельные решения, существование которых вытекает из групповой природы уравнения нулевого приближения (15).

Для строго потенциальных течений уравнения (15) было впервые получено Карманом. Уравнением для звуковой поверхности для стационарных течений будет $\varphi_x = 0$, в сверхзвуковой потоке $\varphi_x > 0$, а в дозвуковом $\varphi_x < 0$. Уравнением характеристических поверхностей $x = x(y,z)$ для стационарных течений будет [4]:

$$\left(\frac{\partial x}{\partial y}\right)^2 + \left(\frac{\partial x}{\partial z}\right)^2 = \frac{\partial \varphi}{\partial x}, \qquad (16)$$

где выражение в правой части зависит от решения $\varphi(x, y, z)$. Отсюда следует, что уравнение (15) имеет гиперболический тип для $\varphi_x > 0$ эллиптический тип, если $\varphi_x < 0$ что соответствует общей теории установившихся трансзвуковых течений.

Пусть для нелинейного уравнения (15) имеем сопловое решение с криволинейной звуковой поверхностью вида

$$\varphi_0(x, y, z) = A_1 x^2 + A_2 x y^2 + A_3 x z^2 + A_4 y^2 z^2 + A_5 y^4 + A_6 z^4 \qquad (17)$$

Определяя все необходимые частные производные и подставляя в уравнение (15), получим

$$(2A_1^2 - A_2 - A_3)x - (A_1 A_2 - 6A_5 - A_4)y^2 + (A_1 A_3 - A_4 - 6A_6)z^2 = 0$$

т. е. имеем незамкнутую систему уравнений:

$$2A_1^2 = A_2 + A_3, \quad A_1 A_2 = 6A_5 + A_4, \quad A_1 A_3 = 6A_6 + A_4, \quad A_1 = k_0. \qquad (18)$$

Дополним эту систему следующими соотношениями:

$$A_3 = PA_2, \quad A_6 = PA_5, \quad A_4 = 2PA_5, \qquad (19)$$

где P - некоторое постоянное число, задающее пространственную геометрию сопла. Ниже покажем, что при решении системы алгебраических уравнений (18, 19) при P = 0 - определяет плоский

случай течения, $P = 1$ - осесимметричный, а при $0 < P < 1$ - течение в канале, сечение которого плоскостью параллельной плоскости OYZ, определяет некоторый эллипс.

Разрешая систему уравнений (18,19) имеем

$$A_1 = k_0, \quad A_2 = \frac{2k_0^2}{P+1}, \quad A_3 = \frac{2P}{P+1}k_0^2, \quad A_4 = \frac{2P}{(P+1)}\frac{2k_0^3}{(2P+3)},$$

$$A_5 = \frac{k_0^3}{(P+1)(2P+3)}, \quad A_6 = \frac{Pk_0^3}{(P+1)(2P+3)} \qquad (20)$$

Для плоского случая при $P = 0$ имеем $A_3 = A_4 = A_6 = 0$, а при $P = 1$ – осесимметричного, имеем $A_2 = A_3$, $A_5 = A_6$, $A_4 = 2A_5 = 2A_6$.

Далее решим линейное неоднородное уравнение (15а), которое состоит из суммы решения его однородного уравнения и частных решений неоднородной части $\varphi_1(x,y,z) = \varphi_{10}(x,y,z) + \varphi_{11}(x,y,z)$ (21)

При этом искомые функции будем искать в формах

$$\varphi_{10}(x,y,z) = B_1x^3 + (B_2y^2 + B_3z^2)x^2 + (B_4y^4 + B_5y^2z^2 + B_6z^4)x + (B_7y^6 + B_8y^4z^2 + B_9y^2z^4 + B_{10}z^6) \qquad (22)$$

$$\varphi_{11}(x,y,z) = B_{11}y^6 + B_{12}y^4z^2 + B_{13}y^2z^4 + B_{14}z^6 + (B_{15}y^4 + B_{16}y^2z^2 + B_{17}z^4)x + (B_{18}y^2 + B_{19}z^2)x^2 \qquad (23)$$

Определяя частные производные φ_{10x}, φ_{10xx}, φ_{10y}, φ_{10yy}, φ_{10z}, φ_{10zz}, φ_{10xy}, φ_{10xz} и подставляя однородную часть уравнения (15а) получим следующую систему

$$9A_1B_1 - B_2 - B_3 = 0 \qquad A_2B_3 + A_3B_2 + A_1B_6 - 6B_{10} - 6A_9 = 0,$$

$$4A_1B_2 + 3A_2B_1 - 6B_5 - B_6 = 0, \qquad A_3B_3 + A_1B_4 - B_9 - 15B_7 = 0,$$

$$4A_1B_3 + 3A_3B_1 - 6B_4 - B_6 = 0, \quad A_2B_2 + A_1B_5 - 15B_8 - B_{10} = 0, \quad B_1 = k_1, \qquad (24)$$

Здесь также определяя все необходимые частные производные, $\varphi_{11}(x,y,z)$ подставляя их в рассматриваемое неоднородное уравнение (15а), получим следующую недоопределенную систему

$$8A_1B_{19} - 2B_{16} - 12B_{17} = 8A_3^2 + 4A_1^2A_3 + 2(\gamma-1)[2A_1(A_4 + 6A_6) + A_3(A_2 + A_3)],$$

$$8A_1B_{18} - 12B_{15} - 8B_{16} = 8A_2^2 + 4A_1^2A_2 + 2(\gamma-1)[A_2(A_2 + A_3) + 2A_1(6A_5 + A_4)],$$

$$2A_2B_{19} - 2A_3B_{18} + 2A_1B_{16} - 12B_{12} - 12B_{13} = 8A_4(A_2 + A_3) + 2A_1A_2A_3 + 2(\gamma-1)[A_2(A_4 + 6A_6) + A_3(6A_5 + A_4)], \qquad (25)$$

$$2A_2B_{18} + 2A_1B_{15} - 30B_{11} - 2B_{12} = 16A_2A_5 + A_1A_2^2 + 2(\gamma-1)A_2(6A_5 + A_4),$$

$$2A_3B_{19} + 2A_1B_{17} - 2B_{13} - 30B_{14} = 16A_3A_6 + A_1A_3^2 + 2(\gamma - 1)A_3(A_4 + 6A_6),$$

$$-B_{18} + B_{19} = 2A_1^3 + 2(\gamma - 1)A_1(A_2 + A_3).$$

Дополняя данную систему следующими соотношениями получим уже определенную систему для определения искомых коэффициентов A_i, $(A_i = 1,2,\ldots 19)$. $\frac{B_3}{B_2} = \frac{B_6}{2B_5} = \frac{B_{10}}{3B_8} = P, \quad \frac{B_{19}}{B_{18}} = \frac{B_{16}}{2B_{15}} = \frac{B_{12}}{3B_{11}} = P$ (26)

С учетом полученных решений можно получить уравнение стенки сопла для пространственного случая в двух приближениях

$$\begin{cases} \bar{y} = \varepsilon\Big\{x^2(A_2y + A_4yz^2 + 2A_5y^3) + \varepsilon\Big[\frac{2}{3}x^3(B_2 + B_{18})y + x^2\big[2(B_5 + B_{15})y^3 + \\ +(B_6 + B_{16})yz^2\big] + x\big[6(B_8 + B_{11})y^5 + 2(B_9 + B_{13})yz^4 + 4(B_{10} + B_{12})y^3z^2\big]\Big] \\ \bar{z} = \varepsilon\big\{x^2(A_3z + A_4y^2z + 2A_6z^6) + \varepsilon\Big[\frac{2}{3}x^3(B_3 + B_{19})z + x^2\big[2(B_4 + B_{17})z^3 + \\ +(B_6 + B_{16})y^2z^2\big] + x\big[6(B_7 + B_{14})z^5 + 2(B_{10} + B_{12})y^4z + 4(B_9 + B_{13})y^2z^3\big]\Big] \end{cases} \quad (27)$$

Здесь $\bar{y}$, $\bar{z}$ - отклонения от прямой, являющейся пересечением плоскостей координатами следующей кривой, $\bar{y} = c_1$ $\bar{z} = c_2$ координатами следующей кривой

$$\varepsilon(A_4y^2z^2 + A_5y^4 + A_6z^4) + \\ +\varepsilon^2\big[(B_8 + B_{11})y^6 + (B_{10} + B_{12})y^4z + (B_9 + B_{13})y^2z^4 + (B_7 + B_{14})z^6\big] = \text{const} \quad (28)$$

Звуковая поверхность с учетом двух приближений запишется как

$$2A_1x + A_2y^2 + A_3z^2 + \varepsilon\big\{3B_1x^2 + 2x\big[(B_2 + B_{18})y^2 + (B_3 + B_{19})z^2\big] + \\ +(B_4 + B_{17})z^4 + (B_5 + B_{16})y^6\big\} = 0. \quad (29)$$

Здесь видно, что звуковая поверхность представляет собой параболу, причем наклонена в сторону набегающего потока. Решение нелинейного уравнения нулевого приближения (15) ищется в форме: (где a_0, b_0 – пока произвольные постоянные для пространственного потока).

$$\varphi(x, y, z) = (a_0y + b_0z)^{3m-2}f(\eta), \quad \eta = \frac{(a_0^2 + b_0^2)x}{(a_0y + b_0z)^m}, \quad (30)$$

Определим частные производные

$$\eta_x = \frac{(a_0^2 + b_0^2)x}{(a_0y + b_0z)^m}, \quad \eta_y = -\frac{(a_0^2 + b_0^2)a_0mx}{(a_0y + b_0z)^{m+1}} = -\frac{a_0m\,\eta}{(a_0y + b_0z)}, \quad \eta_z = -\frac{b_0m\,\eta}{(a_0y + b_0z)}.$$

$$\varphi_{0x} = (a_0^2 + b_0^2)(a_0y + b_0z)^{2m-2}f',$$

$$\varphi_{0xx} = (a_0^2 + b_0^2)^2(a_0y + b_0z)^{m-2}f''.$$

$$\varphi_{0y} = (3m-2)(a_0y+b_0z)^{3m-3}a_0f - a_0m(a_0y+b_0z)^{3m-3}\eta\cdot f';$$

$$\varphi_{0yy} = a_0^2(3m-2)(3m-3)(a_0y+b_0z)^{3m-4}f +$$

$$+(a_0y+b_0z)^{3m-4}\left[a_0^2m^2-(3m-2)a_0^2m-(3m-3)a_0^2m\right]\eta f' + a_0^2m^2(a_0y+b_0z)^{3m-4}\eta^2 f'',$$

$$\varphi_{0zz} = b_0^2(3m-2)(3m-3)(a_0y+b_0z)^{3m-4}f +$$

$$+(a_0y+b_0z)^{3m-4}\left[m^2-(3m-2)m-(3m-3)m\right] b_0^2\eta f' + b_0m^2(a_0y+b_0z)^{3m-4}\eta^2 f'',$$

и подставляя в уравнение (15), получим следующее обыкновенное нелинейное дифференциальное уравнение

$$\left[m^2\eta^2-(a_0^2+b_0^2)^2f'\right]f''-5m(m-1)\eta f'+(3m-2)(3m-3)f=0 \qquad (31)$$

Одно из частных решений (31) можно найти как $f(\eta)=P_1\eta^2+P_2\eta+P_3$ Действительно, дифференцируя его два раза и подставляя в уравнение (31), получим (где $P_1=P_0/(a_0^2+b_0^2)^2$)

$$\varphi(x,y,z) = P_0x^2 + \frac{2P_0^2x(a_0y+b_0z)^2}{(a_0^2+b_0^2)} + \frac{P_0^3(a_0y+b_0z)^4}{3(a_0^2+b_0^2)^2}, \qquad (32)$$

Если сравнить полученное решение (32) с ранее полученным сопловым решением с криволинейной звуковой поверхностью (17), то убеждаемся, что $A_1=P_0$, то есть решение уравнения (32) является более общим чем (17).

СПИСОК ЛИТЕРАТУРЫ

1 **Кочин, Н. Е., Кибель, Н. А., Розе, Н. В.** Теоретическая гидромеханика. – М., физмат., 1963.

2 **Ландау, Л. Д., Лифшиц, Е. М.** Механика сплошных сред. – М., 1954.

3 **Рыжов, О. С.** Исследование трансзвуковых течений в соплах Лаваля. – М. : Изд-во ВЦ АН СССР, 1965. – 238 с.

4 **Курант, Р., Гильберт, Д.** Мстоды математической физики. – Т. 2. – М.- Л. : ГИТТЛ, 1951.

Кыргызский национальный аграрный университет
имени К. И. Скрябина, г. Бишкек. Кыргызская Республика.

Материал поступил в редакцию 02.06.13.

А. Т. Дыйканова

Түтіктің ішіндегі сұйықтықтың сығылғыштығының ағымының дыбыс маңындағы стационарлық есебі

К. И. Скрябин атындағы Қырғыз ұлттық аграрлық университеті,
Бишкек қ., Қырғыз Республикасы.
Материал 02.06.13 редакцияға түсті.

A. T. Dyikanova

The stationary problem of transonic compressible flow of fluid in the nozzles

National Agrarian University named after K. I. Skryabin,
Bishkek, Kyrgyzstan.
Material received on 02.06.13.

Жұмыста түтіктің ішіндегі газдың ағымының құйынсыздықтың стационарлық есебі қаралды және зерттелінді.

In the article are considered and investigated dimensional stationary problem irrotational flow of gas in the nozzles.

УДК 515.12

Т. Ж. Жумалиев

КАРДИНАЛЬНЫЕ ИНВАРИАНТЫ РАВНОМЕРНЫХ ПРОСТРАНСТВ

В данной статье изучаются μ-полные и μ-пополнение равномерных пространств, а также, равномерно непрерывные отображения μ- полных равномерных пространств.

Рассмотрим некоторые необходимые для дальнейшего изложения понятия топологических, равномерных пространств и равномерно непрерывных отображений.

Пусть (X,U)- равномерное пространство, а $\mathcal{F}$- фильтр в X. Фильтр $\mathcal{F}$ называется фильтром Коши в (X,U), если $\alpha \cap \mathcal{F} \neq \emptyset$ для любого $\alpha \in U$.

Пусть (X,τ)- топологическое пространство. Фильтр $\mathcal{F}$ в X называется фильтром окрестностей точки x в (X,τ), если внутренность каждого элемента фильтра $\mathcal{F}$ содержит точку x. Говорят, что фильтр $\mathcal{F}$ сходится в (X,τ) к точке x, если $\mathcal{F}$ сильнее, чем фильтр окрестностей точки x, т. е. любой элемент фильтра $\mathcal{F}$ является окрестностью точки x. Фильтр $\mathcal{F}$ в равномерном пространстве (X,U) называется сходящимся к точке $x \in X$, а точка x-пределом фильтра $\mathcal{F}$, если он сходится к точке $x \in X$ в (X,τ_U). Точка $x \in X$ называется точкой прикосновения фильтра $\mathcal{F}$ в (X,U), если x является точкой прикосновения каждого элемента фильтра $\mathcal{F}$ в (X,τ_U), где (X,τ_U)-топологическое пространство, порожденное равномерным пространством (X,U).

Минимальные по включению элементы множества всех фильтров Коши в равномерном пространстве (X,U) называются минимальными фильтрами Коши в (X,U).

Равномерное пространство называют полным, если всякий фильтр Коши в нем сходится.

Пусть α- покрытие множества X. Положим $\alpha^{\vee} = \{\cup\, \alpha' : \alpha' - \text{конечноеподмножество покрытия}\alpha\}$.

ОПРЕДЕЛЕНИЕ (Б.А. Пасынков). Равномерно непрерывное отображение $f:(X,U) \to (Y,V)$ равномерного пространства (X,U) на равномерное пространство (Y,V) называется дважды равномерно непрерывным, если для любого $\alpha \in U$ существует такое $\beta \in V$ что покрытие $f^{-1}\beta$ вписано в покрытие $\alpha^{\vee}$.

Непрерывное отображение f топологического пространства X в топологическое пространство Y называется совершенным, если оно замкнуто и для всякой точки $y \in Y$ ее прообраз $f^{-1}y$ компактен.

Пусть (X,U)- произвольное равномерное пространство а μ- некоторос кардинальное число. Через $\omega(U)$ обозначим вес равномерного пространства (X,U)

ОПРЕДЕЛЕНИЕ (А.А. Борубаев). Равномерное пространство (X,U) называется μ- полным, если всякий фильтр Коши $\mathcal{F}$, имеющий базу B мощностью $|B| \le \mu$ сходится, где $\tau = \omega(U)$ и $\aleph_0 \le \mu \le \tau$.

При $\mu = \aleph_0$ равномерное пространство (X,U) называется секвенциально полным, а при $\mu = \tau$ называется полным.

ОПРЕДЕЛЕНИЕ (А.А. Борубаев). Равномерное пространство $(\tilde{X}_\mu, \tilde{U}_\mu)$ называется μ- пополнением равномерного пространства (X,U), если:

$X \subset \tilde{X}_\mu$;

(X, τ_U) всюду плотно в $(\tilde{X}_\mu, \tau_{\tilde{U}_\mu})$;

$(\tilde{X}_\mu, \tilde{U}_\mu)$- μ- полное равномерное пространство.

Следующая теорема дает μ- пополнения равномерного пространства.

ТЕОРЕМА 1. Для каждого равномерного пространства (X,U) существует единственное, с точностью до равномерного изоморфизма, μ- пополнение $(\tilde{X}_\mu, \tilde{U}_\mu)$.

Покажем конструкцию доказательств теоремы. Пусть $\tilde{X}_\mu$- множество всех минимальных фильтров Коши, имеющий базу B мощностью $|B| \le \mu$ в (X,U). Для каждого $\alpha \in U$ положим $\tilde{\alpha} = \{\tilde{A}: A \in \alpha\}$, где $\tilde{A} = \{\mathcal{F} \in \tilde{X}_\mu; A \in \mathcal{F}\}$. Доказывается, что $\tilde{\alpha}$- покрытие множества $\tilde{X}_\mu$. Положим $\tilde{B} = \{\tilde{\alpha}: \alpha \in U\}$. Тогда $\tilde{B}$- является базой мощностью $|\tilde{B}| \le \mu$ некоторой равномерности $\tilde{U}_\mu$ в $\tilde{X}_\mu$.

Показывается, что равномерное пространство (X,U) равномерно изоморфно некоторому равномерному подпространству μ- полного пространства $(\tilde{X}_\mu, \tilde{U}_\mu)$. Определяется отображение $i: X \to \tilde{X}_\mu$ и что отображение i взаимно однозначно.

Доказывается, что равномерное пространство $(\tilde{X}_\mu, \tilde{U}_\mu)$- μ- полно и строится единственность равномерного пространства $(\tilde{X}_\mu, \tilde{U}_\mu)$.

ТЕОРЕМА 2. Пусть $f:(X,U)\to(Y,V)$ - дважды равномерно непрерывное отображение. Тогда, если равномерное пространство (X,U)- μ- полно, то равномерное пространство (Y,V) также μ- полно.

ДОКАЗАТЕЛЬСТВО. Пусть (X,U)-μ- полное равномерное пространство и пусть $f:(X,U)\to(Y,V)$ - дважды равномерно непрерывное отображение. Покажем, что (Y,V) также является μ-полным. Пусть $\mathcal{F}_Y$- произвольный фильтр Коши равномерного пространства (Y,V), имеющий базу мощности $\leq \mu$. Через γ обозначим ультрафильтр в X содержащий семейство $f^{-1}\mathcal{F}_Y$. Найдется $\tilde{A}\in\alpha^\vee\cap\gamma$ для любого $\alpha\in U$. Пусть $\tilde{A}=\bigcup_{i=1}^n A_i$, $A_i\in\alpha$. Так как γ ультрафильтр и $\bigcup_{i=1}^n A_i\in\gamma$, то $A_i\in\gamma$ для некоторого $i=1,2,\dots,n$. Это означает, что ультрафильтр γ является фильтром Коши. В силу μ-полноты равномерного пространства (X,U), фильтр Коши γ которая имеет базу мощностью $\leq\mu$ сходится к некоторой точке $x\in X$. Следовательно, фильтр $f(\gamma)$ сходится к точке fx и можорирует фильтр Коши $\mathcal{F}_Y$. Поэтому точка x является точкой прикосновения фильтра $\mathcal{F}_Y$. Следовательно, равномерное пространство (Y,V) является μ- полным.

СЛЕДСТВИЕ (Б.А. Пасынков [4]). Если $f:(X,U)\to(Y,V)$ - дважды равномерно непрерывное отображение, то из полноты равномерного пространства (X,U) следует полнота равномерного пространства (Y,V).

ТЕОРЕМА 3. Пусть $f:(X,U)\to(Y,V)$- совершенное равномерно непрерывное отображение равномерного пространства (X,U) на μ-полное равномерное пространство (Y,V). Тогда равномерное пространство (X,U) также μ- полно.

ДОКАЗАТЕЛЬСТВО. Пусть (Y,V)- μ- полное равномерное пространство. Покажем, что пространство (X,U) является μ- полным.

Пусть $\mathcal{F}$- произвольный фильтр Коши в (X,U) имеющий базу мощности $\leq \mu$. Тогда $f\mathcal{F}$ является фильтром Коши в (Y,V) и легко видеть, что оно имеет базу мощности $\leq \mu$. Так как (Y,V)- μ- полно, то он сходится к некоторой точке пространства (Y,V). В силу совершенности отображения f, заключаем, что фильтр $\mathcal{F}$ сходится к некоторой точке. Значит, равномерное пространство (X,U) является μ- полным.

СЛЕДСТВИЕ (А.А. Борубаев [3]). Если $f:(X,U)\to(Y,V)$- совершенное равномерно непрерывное отображение равномерного пространства (X,U) на полное равномерное пространство (Y,V), то следует, что равномерное пространство (X,U) также полно.

ТЕОРЕМА 4. Пусть $f:(X,U)\to(Y,V)$- дважды равномерно непрерывное совершенное отображение. Если одно из равномерных пространств (X,U) и (Y,V) μ- полно, то и другое равномерное пространство также μ- полно.

Доказательство следует из теоремы 2 и теоремы 3.

СЛЕДСТВИЕ (А.А. Борубаев [2]). Если $f:(X,U)\to(Y,V)$- дважды равномерно непрерывное совершенное отображение и одно из равномерных пространств (X,U) и (Y,V) полно, то и другое равномерное пространство также полно.

Пусть $\{(X_m,U_m): m\epsilon M\}$- семейства равномерных пространств.

ТЕОРЕМА 5. Пусть $\{(X_m,U_m): m\epsilon M\}$- такое семейство равномерных пространств, что (X_m,U_m)-μ_m-полно. Тогда произведение $\prod\{(X_m,U_m): m\epsilon M\}$- любого семейства равномерных пространств μ- полно, где $\mu = sup\{\mu_m: m\epsilon M\}$.

ДОКАЗАТЕЛЬСТВО. Пусть $(X,U)=\prod\{(X_m,U_m): m\epsilon M\}$- произведение семейства μ - полных равномерных пространств $\{(X_m,U_m): m\epsilon M\}$, а $\mathcal{F}$- фильтр Коши в (X,U) имеющий базу мощностью $\leq \mu$. Положим $\mathcal{F}_m=\pi_m(\mathcal{F})$, где $\pi_m: X\to X_m$- проекция X на m- й сомножитель X_m, которая является равномерно непрерывной

по определению произведения равномерностей. Так как пространство (X_m, U_m)- μ_m- полно, то существует $\mathcal{F}_m$- фильтр Коши имеющего базу мощностью $\leq \mu$ в (X_m, U_m), где $\mu = sup\{\mu_m : m \epsilon M\}$. Из того, что отображение π_m сюръективное («на») $\mathcal{F} = \pi^{-1}\mathcal{F}_m$ фильтр в (X, U). Теперь покажем, что $\mathcal{F}-$ фильтр Коши имеющего базу мощностью $\leq \mu$. Пусть γ- произвольное покрытие пространства (X, τ_U). Определим, что $\gamma = \gamma_{m_1} \times ... \times \gamma_{m_n} \times \prod\{X_m : m \epsilon M \setminus \{m_1, ..., m_n\}\}$, где γ_{m_i}- покрытие в $\left(X_{m_i}, \tau_{U_{m_i}}\right)$, $i = 1,2, ..., n$. Так как $\gamma_{m_i} \in \mathcal{F}_{m_i}$, $i = 1,2, ..., n$, то $\gamma = \cap_{i=1}^{n} \pi_{m_i} \gamma_{m_i} \in \mathcal{F}$ и оно сходится к некоторой точке (X, τ_U). Значит, (X, U)- μ- полное равномерное пространство.

СЛЕДСТВИЕ (А. Вейль [1]). Произведение любого множества полных равномерных пространств, является полным равномерным пространством.

Рассмотрим о μ- полноте и μ- пополнении равномерно непрерывных отображений.

Пусть $f: (X, U) \to (Y, V)$ - равномерно непрерывное отображение. Если $\mathcal{F}$ фильтр Коши, имеющий базу B мощностью $|B| \leq \mu$ в (X, U), то $f\mathcal{F} = \{fF : F \in \mathcal{F}\}$ является фильтром Коши имеющий базу, мощностью $\leq \mu$ в (Y, V). База фильтра Коши $f\mathcal{F}$ мощностью $\leq \mu$, сходится к точке $y \in Y$, если для всякой окрестности O_y точки y найдется $fF \in f\mathcal{F}$ такой, что $fF \subset O_y$.

ОПРЕДЕЛЕНИЕ (А.А. Борубаев). Пусть $f: (X, U) \to (Y, V)$ - равномерно непрерывное отображение равномерного пространства (X, U) в равномерное пространство (Y, V) называется μ- полным, если всякий фильтр Коши $\mathcal{F}$, имеющий базу мощностью $\leq \mu$ в (X, U), для которого $f\mathcal{F}$ сходится в (Y, V), сходится в (X, U).

Рассмотрим следующий квадрат категории *Unif*:

$$\begin{array}{ccc} (X, U) & \xrightarrow{i_X} & (\tilde{X}_\mu, \tilde{U}_\mu) \\ f \downarrow & & \downarrow \tilde{f}_\mu \\ (Y, V) & \xrightarrow{i_Y} & (\tilde{Y}_\mu, \tilde{V}_\mu), \end{array}$$

где $(\tilde{X}_\mu, \tilde{U}_\mu)$ и $(\tilde{Y}_\mu, \tilde{V}_\mu)$- μ- пополнения равномерных пространств (X,U) и (Y,V), соответственно, $\tilde{f}_\mu$- равномерно непрерывное продолжение f на $(\tilde{X}_\mu, \tilde{U}_\mu)$ и $(\tilde{Y}_\mu, \tilde{V}_\mu)$, соответственно, а i_X и i_Y - тождественные равномерные вложения равномерных пространств (X,U) и (Y,V) в $(\tilde{X}_\mu, \tilde{U}_\mu)$ и $(\tilde{Y}_\mu, \tilde{V}_\mu)$, соответственно. Можно видеть, что квадрат является коммутативным.

ТЕОРЕМА 6. Для равномерно непрерывного отображения $f: (X,U) \to (Y,V)$ равномерного пространства (X,U) на равномерное пространство (Y,V) следующие условия равносильны:

Отображение f μ- полно;

$$\tilde{f}_\mu(\tilde{X}_\mu \backslash X) \subset \tilde{Y}_\mu \backslash Y;$$

Квадрат декартов в категории *Unif*.

ДОКАЗАТЕЛЬСТВО. 1)→2). Пусть $f: (X,U) \to (Y,V)$ - μ- полное отображение, а $y \notin \tilde{Y}_\mu \backslash Y$. Тогда $y \in Y$. Пусть $x \in X$- такая точка, что $\tilde{f}_\mu(x) = y$. Если $x \in X$, то $x \notin \tilde{X}_\mu \backslash X$ и $y \notin \tilde{f}_\mu(\tilde{X}_\mu \backslash X)$. Включение $\tilde{f}_\mu(\tilde{X}_\mu \backslash X) \subset \tilde{Y}_\mu \backslash Y$ доказано. Предположим, что $x \in \tilde{X}_\mu \backslash X$. Через $\mathcal{F}$ обозначим след на X фильтра окрестностей точки x. Тогда $\mathcal{F}$- фильтр Коши, имеющий базу B мощностью $|B| \le \mu$ в (X,U). Если его образ $f\mathcal{F}$ сходится к точке $y \in Y$, то f - μ- полное отображение, т. е. фильтр Коши $\mathcal{F}$, имеющий базу B мощностью $|B| \le \mu$ сходится к некоторой точке $x_1 \in X$. Но по определению фильтра $\mathcal{F}$, он не имеет предела в (X,U), его предел $x = x_1$ лежит вне пространства X. Пришли к противоречию. Поэтому единственно возможно $x \in X$ и включение $\tilde{f}_\mu(\tilde{X}_\mu \backslash X) \subset \tilde{Y}_\mu \backslash Y$ доказано.

2) → 3). Пусть $\tilde{f}_\mu(\tilde{X}_\mu \backslash X) \subset \tilde{Y}_\mu \backslash Y$, $\varphi: (Z,W) \to (Y,V)$ и $\psi: (Z,W) \to (\tilde{X}_\mu \backslash X)$ такие равномерно непрерывные отображения, что $i_Y \circ \varphi = \tilde{f}_\mu \circ \psi$. Учитывая, что i_X и i_Y - тождественные равномерные вложения, $i_Y(\varphi(Z))$ содержится в $\tilde{Y}_\mu$. Из вложения $\tilde{f}_\mu(\tilde{X}_\mu \backslash X) \subset \tilde{Y}_\mu \backslash Y$ и

равенства $\tilde{f}(\psi(Z)) = i_Y(\varphi(Z))$ следует, что $\varphi(Z) \subset X$. Определим отображение $h: Z \to X$ по правилу $h(z) = \psi(z)$ для любого $z \in Z$. По определению отображения h, имеем $\psi = i_X \circ h$ и $\varphi = f \circ h$. Покажем, что $h: (Z,W) \to (X,U)$ равномерно непрерывно. Так как на $\varphi(Z)$ равномерности U и $\widetilde{U}_\mu$ индуцируют одинаковую равномерность, то из равномерной непрерывности отображения ψ следует равномерная непрерывность отображения h. Единственность отображения h следует из его определения. Следовательно, квадрат декартов в категории *Unif*.

3) $\to$ 1). Пусть квадрат декартов в категории *Unif*, а $\mathcal{F}$- фильтр Коши имеющий базу мощностью $\leq \mu$ в (X,U) такой, что $f\mathcal{F}$ сходится к точке $y \in Y$ в (Y,V). Тогда фильтр Коши $\mathcal{F}$ имеющий базу мощностью $\leq \mu$ в (X,U) является базисом фильтра в $(\tilde{X}_\mu, \tilde{U}_\mu)$ и поэтому сходится к некоторой точке $x \in \tilde{X}_\mu$. Покажем, что $x \in X$. Рассмотрим одноточечное равномерное пространство $Z = \{x\}$ с тривиальной равномерностью W. Введем отображение $\varphi: (Z,W) \to (Y,V)$ и $\psi: (Z,W) \to (\tilde{X}_\mu, \tilde{U}_\mu)$ так, чтобы $\varphi(x) = y$ и $\psi(x) = x$. Так как $\tilde{f}_\tau(x) = y$ то $i_X \circ \varphi = \tilde{f}_\tau \circ \psi$. Поэтому существует единственное отображение $h: (Z,W) \to (X,U)$ такое, что $\psi = i_X \circ h$ и $\varphi = f \circ h$. Но $i_X(h(x)) = \psi(x)$, $x \in X$, т. е. $\mathcal{F}$- фильтр Коши имеющий базу мощностью $\leq \mu$ сходится в (X,U) и равномерно непрерывное отображение $f: (X,U) \to (Y,V)$- μ- полно. Теорема доказано.

ОПРЕДЕЛЕНИЕ. Пусть $f: (X,U) \to (Y,V)$ - равномерно непрерывное отображение равномерного пространства (X,U) в равномерное пространство (Y,V). Равномерно непрерывное отображение $\hat{f}: (\hat{X},\hat{U}) \to (Y,V)$ равномерного пространства $(\hat{X},\hat{U})$ в равномерное пространство (Y,V) называется μ- пополнением отображения f, если выполняются следующие условия:

Равномерное пространство (X,U) есть всюду плотное подпространство равномерного пространства $(\hat{X},\hat{U})$;

$$f = \hat{f}\,|_X;$$

Отображение $\hat{f}$ является μ- полным.

ТЕОРЕМА 7. Всякое равномерно непрерывное отображение $f: (X,U) \to (Y,V)$ равномерного пространства (X,U) в равномерное пространство (Y,V) имеет единственное, с точностью до равномерного изоморфизма, μ- пополнение.

ДОКАЗАТЕЛЬСТВО. Пусть $(\tilde{X}_\mu, \tilde{U}_\mu)$ и $(\tilde{Y}_\mu, \tilde{V}_\mu)$- μ- пополнения равномерных пространств (X,U) и (Y,V), соответственно, а $\tilde{f}_\mu: (\tilde{X}_\mu, \tilde{U}_\mu) \to (\tilde{Y}_\mu, \tilde{V}_\mu)$- единственное равномерно непрерывное продолжение отображения f. Положим $\hat{X} = \tilde{f}_\mu^{-1}Y$ и $\hat{f} = \tilde{f}_\mu\,|_{\hat{X}}$. Тогда $X \subset \hat{X}$ и $\hat{f}\,|_X = f$. Пусть $\hat{U}$- равномерность на $\hat{X}$, индуцированная равномерностью $\tilde{U}_\mu$. Тогда очевидно, что отображение $\hat{f}: (\hat{X}, \hat{U}) \to (Y,V)$ является равномерно непрерывным. Равномерное пространство $(\tilde{X}_\mu, \tilde{U}_\mu)$ является μ- пополнением пространства $(\hat{X}, \hat{U})$, и из единственности отображения $\tilde{f}_\mu$ следует, что отображение $\hat{f}$ является единственным равномерно непрерывным продолжением отображения f на пространство $(\hat{X}, \hat{U})$ имеем $\tilde{f}_\mu(\tilde{X}_\mu \backslash X) \subset \tilde{Y}_\mu \backslash Y$. Тогда, отображение $\hat{f}$ - μ- полно.

СПИСОК ЛИТЕРАТУРЫ

1 **Энгелькинг, Р.** Общая топология. – Москва : Мир, 1986.

2 **Борубаев, А. А.** Равномерные пространства и равномерно непрерывные отображения. – Фрунзе : Илим, 1990.

3 **Борубаев, А. А., Чекеев А. А.** Равномерные пространства. – Бишкек: Учкун, 2003.

4 **Пасынков, Б. А.** О топологических группах. – Доклады Академии наук СССР. –Том 188, №2, 1969.

Кыргызский национальный аграрный университет
имени К. И. Скрябина, г. Бишкек, Кыргызская Республика.
Материал поступил в редакцию 04.06.13.

Т. Ж. Жумалиев

Бірқалыпты кеңістіктердің кардиналдық инварианттары

К. И. Скрябин атындағы Қырғыз ұлттық аграрлық
университеті, Бишкек қ., Қырғыз Республикасы.
Материал 04.06.13 редакцияға түсті.

T. J. Jumaliev

The cardinal invariants of regular spaces

National Agrarian University named after
K. I. Skryabin, Bishkek, Kyrgyzstan.
Material received on 04.06.13.

Бұл мақалада μ- толық және μ- бірқалыпты кеңістіктерді толықтыру, сонымен қатар, μ-толық толық бірқалыпты кеңістіктердің бірқалыпты үзіліссіз шағылуы зерттеледі.

Regular spaces μ-completeness and μ-completion as well as regular representation of reflection and regular spaces have been described in this article.

УДК 539.3:534.2

Н. А. Испулов, А. К. Сейтханова

О МАТРИЧНОЙ ФОРМУЛИРОВКЕ ЗАДАЧ ОТРАЖЕНИЯ – ПРЕЛОМЛЕНИЯ ТЕРМОУПРУГИХ ВОЛН

Актуальность исследования закономерностей волновых процессов в упругих средах с термомеханическим эффектом связана с необходимостью решения теоретических и прикладных задач геофизики, сейсмологии, механики композитных материалов и т.д. Связанные уравнения движения и уравнения

теплопроводности отличаются сложностью и обилием физико-механических параметров. В связи с этим интенсивно развивается раздел механики деформируемого твердого тела, - термоупругость. В рамках этого направления, опираясь на использование определенных физико-механических свойств анизотропных средах, изучаются связанные тепловые и механические поля.

В данной статье приведена матричная формулировка задач отражения – преломления термоупругих волн на границах раздела различных сред.

Термоупругость описывает широкий круг явлений, являясь обобщением теорий упругости и теплопроводности. Принципиально важным является связанность полей деформации и температуры.

Пусть границей раздела двух однородных анизотропных полупространств является плоскость z=0. Прямые и обратные волны в этих средах задаются матрицантами прямых (T^+) и обратных (T^-) волн. Матрицанты первой среды обозначим через T_1^+ и T_1^-, а матрицант прямых волн второй среды через T_2^+. Матричная постановка и решение данной задачи сводится к следующему.

Падающие, отраженные и преломленные волны задаются в виде [1,2]:

$$\vec{w}_{пад} = T_1^+ \vec{w}_0 \tag{1}$$

$$\vec{w}_{отр} = T_1^- \vec{w}_r \tag{2}$$

$$\vec{w}_{пр} = T_2^+ \vec{w}_t \tag{3}$$

где вектора $\vec{w}_{пад}$, $\vec{w}_{отр}$, $\vec{w}_{пр}$ – содержат смещения точек среды u_z, u_x, u_y компоненты тензора напряжений σ_{zz}, σ_{xz}, σ_{yz} и компоненты теплового поля θ, q_z; T_1^+, T_1^- и T_2^+ определяются через соответствующие матрицы коэффициентов, т. е. содержат физико-механические параметры сред, частоту, и, x и y компоненты волновых векторов; $\vec{w}_0$ – вектор определяющий амплитуды падающих волн; $\vec{w}_r$ – вектор определяющий амплитуды отраженных волн; $\vec{w}_t$ – вектор определяющий амплитуды преломленных волн.

На границе должны выполняться условия:

$$\vec{w}_{пад}(0) = T_1^+(0)\vec{w}_0 = \vec{w}_0 \tag{4}$$

$$\vec{w}_{отр}(0) = T_1^-(0)\vec{w}_r = \vec{w}_r \tag{5}$$

$$\vec{w}_{пр}(0) = T_2^+(0)\vec{w}_t = \vec{w}_t \tag{6}$$

Из (4)-(6) становиться ясным физический смысл векторов $\vec{w}_0$, $\vec{w}_r$, $\vec{w}_t$. Это вектора определяющие смещения точек среды (u_z, u_x, u_y), компоненты тензора напряжений (σ_{zz}, σ_{xz}, σ_{yz}), а также компоненты теплового поля (θ, q_z) на границе раздела сред. Условия (4)-(6) также связывают между собой значения на границе раздела смещения u_z и компоненту напряжения σ_{zz}, смещения u_x и компоненту напряжения σ_{xz}, смещения u_y и компоненту напряжения σ_{yz}, а также θ и q_z.

Для решения задачи отражения волн необходимо записать граничные условия. Так как в векторы столбцы входят смещения, нормальные к границе компоненты напряжения и касательные к границе составляющие теплового поля, то первое условие (4) запишется следующим естественным образом:

$$\vec{w}_0 + \vec{w}_r = \vec{w}_t \tag{7}$$

Помимо этого условия ставится матричное условие, которое является следствием непрерывности решений:

$$T_1^+(0)\vec{w}_0 + T_1^-(0)\vec{w}_r = T_2^+(0)\vec{w}_t \tag{8}$$

Решая совместно (7) и (8) для векторов $\vec{w}_r$ и $\vec{w}_t$ получим:

$$\vec{w}_r = (T_2^+(0) - T_1^-(0))^{-1}(T_1^+(0) - T_2^+(0))\vec{w}_0 \tag{9}$$

$$\vec{w}_t = \left[E + (T_2^+(0) - T_1^-(0))^{-1}(T_1^+(0) - T_2^+(0))\right]\vec{w}_0 \tag{10}$$

Введем обозначение

$$G = (T_2^+(0) - T_1^-(0))^{-1}(T_1^+(0) - T_2^+(0)) \tag{11}$$

Тогда (9) и (10) можно переписать

$$\vec{w}_r = G\vec{w}_0 \tag{12}$$

$$\vec{w}_t = \left[E + G\right]\vec{w}_0 \tag{13}$$

Таким образом, из (2)-(3), (9)-(10) поля отраженных и преломленных волн запишутся в виде:

$$\vec{w}_{отр} = T_1^- G \vec{w}_0 \tag{14}$$

$$\vec{w}_{пр} = T_2^+ (E+G)\vec{w}_0 \tag{15}$$

Выражения (14) и (15) являются решениями поставленной задачи. Из выражения (11) видно, что матрица G определяется матрицантами прямых и обратных волн при z=0.

Матрицанты прямых и обратных волн при z=0 равны:

$$T^{\pm}(0) = \frac{1}{2}(E \pm i\alpha R) \tag{16}$$

где

$$\alpha = \frac{1}{k\kappa(k+\kappa)} \tag{17}$$

$$R = \langle B \rangle^3 + (\alpha + \frac{1}{2}\sqrt{\alpha^2 - \Delta^2}\,)\langle B \rangle \tag{18}$$

Связанные уравнения термоупругости отличаются обилием упругих и термомеханических параметров. В связи с этим, в настоящее время, матричные методы являются наиболее конструктивными и эффективными.

В рамках метода матрицанта усредненный матрицант, описывающий распространение связанных гармонических термоупругих волн в анизотропных средах с термомеханическим эффектом имеет вид [3]:

$$T^{\pm}_{уср} = \left(\pi + \frac{1}{2}E\right)\left(E\cos kz \pm \frac{B}{k}\sin kz\right) - \left(\pi - \frac{1}{2}E\right)\left(E\cos \chi z \pm \frac{B}{\chi}\sin \chi z\right) \tag{19}$$

$$\frac{d\vec{W}}{dz} = B\vec{W} \qquad \vec{W} = \left(U_z, \sigma_{zz}, U_x, \sigma_{xz}, U_y, \sigma_{yz}, \theta, q_z\right)$$

Матрицы π, P определяются формулами:

$$\pi = \frac{P - \tilde{P}_2 E}{\tilde{P}_1 - \tilde{P}_2} - \frac{1}{2}E \;; \qquad P = E + \frac{B_0^2 h^2}{2} \tag{20}$$

$\vec{W}$ - вектор, содержащий компоненты упругих и тепловых полей,

θ - приращение температуры, q_z - поток тепловой энергии.

$\widetilde{P}_1, \widetilde{P}_2$ являются корнями характеристического уравнения следующих из условия [4]:

$$\det(P - \lambda E) = 0$$

Значения волновых чисел k и χ определяются из разложения соответствующих уравнений дисперсии термоупругих волн. В данном случае они имеют вид:

$$1 - \frac{k^2 h^2}{2} = \widetilde{P}_1; \qquad 1 - \frac{\chi^2 h^2}{2} = \widetilde{P}_2 \tag{21}$$

В $\widetilde{P}_1$ и $\widetilde{P}_2$ в соответствии с (20) сохранены члены вплоть до ω^2.

Рассмотрим одномерное распространение термоупругих волн в анизотропной среде тетрагональной сингонии классов 4, $\bar{4}$, 4/m с матрицей коэффициентов B в виде:

$$B = \begin{pmatrix} 0 & b_{12} & b_{17} & 0 \\ b_{21} & 0 & 0 & 0 \\ 0 & 0 & 0 & b_{78} \\ 0 & -i\omega b_{17} & b_{87} & 0 \end{pmatrix} \tag{22}$$

где $b_{12} = \frac{1}{c_{33}}$, $b_{17} = \frac{(2\beta_{13} + \beta_{33})}{c_{33}}$, $b_{21} = -\omega^2 \rho$,

$b_{87} = -i\omega\left(\frac{\beta_{33}^2}{c_{11}} + \frac{c_\varepsilon}{T_0}\right)$, $b_{78} = -\frac{1}{\lambda_{33}}$.

Здесь c_{11}, c_{33} – упругие модули, ρ – плотность среды, λ_{33} – коэффициент теплопроводности, c_ε – теплопроводность при постоянной деформации, β_{13}, β_{33} – термомеханические коэффициенты.

С учетом затухания термоупругих волн, волновые числа k и χ могут быть представлены:

$k = k_0 - ik_1$; $\qquad \chi = \chi_0 - i\chi_1$; $\qquad z \to +\infty$

k_1, χ_1 - коэффициенты затухания упругих и тепловых волн.

Для волн распространяющихся вдоль положительной оси Z из (19) получен матрицант:

$$T_0^{+} = \frac{1}{2}\left(\pi + \frac{1}{2}E\right)\left(E - \frac{B_0}{ik}\right)e^{-ikz} - \frac{1}{2}\left(\pi - \frac{1}{2}E\right)\left(E - \frac{B_0}{i\chi}\right)e^{-i\chi z} \qquad (23)$$

Обратные волны (распространения в область $z<0$; $z\to-\infty$) описываются матрицантом имеющим аналогичное представление:

$$T_0^{-} = \frac{1}{2}\left(\pi + \frac{1}{2}E\right)\left(E + \frac{B_0}{ik}\right)e^{-ikz} - \frac{1}{2}\left(\pi - \frac{1}{2}E\right)\left(E + \frac{B_0}{i\chi}\right)e^{-i\chi z} \qquad (24)$$

Граничные условия. Рассмотрим контакт двух термоупругих полупространств. При z=0 матрицанты (23) и (24) могут быть представлены в виде:

$$T_0^{\pm} = \frac{1}{2}E \mp R; \qquad (25)$$

где

$$R = \frac{1}{2i}\left(\frac{k-\chi}{k\chi}\right)\pi B - \frac{1}{4i}\left(\frac{k+\chi}{k\chi}\right)B$$

Пусть $\vec{W}_0$- поле падающих волн, $\vec{W}_R$- отраженных и $\vec{W}_t$- преломленных волн. Тогда:

$$T_0^{+}\vec{W}_0 + T_0^{-}\vec{W}_R = T_t\vec{W}_t, \text{ при z=0} \qquad (26)$$

или

$$\left(\frac{1}{2}E - R_0\right)\vec{W}_0 + \left(\frac{1}{2}E + R_0\right)\vec{W}_R = \left(\frac{1}{2}E - R_t\right)\vec{W}_t \qquad (27)$$

Учитывая непрерывность полей на контакте сред (7), получим:

$$R_0\vec{W}_0 - R_0\vec{W}_R = R_t\vec{W}_t \qquad (28)$$

С учетом (27) выражение (28) есть искомое граничное условие для векторов $\vec{W}_0, \vec{W}_R, \vec{W}_t$ в матричной форме.

В (7) и (28) неизвестны вектора $\vec{W}_R$ и $\vec{W}_t$. Подстановка (7) в (28) дает уравнение:

$$(R_0 + R_t)\vec{W}_R = (R_0 - R_t)\vec{W}_0 \qquad (29)$$

откуда следует формула для поля отраженных волн $\vec{W}_R$:

$$\vec{W}_R = (R_0 + R_t)^{-1}(R_0 - R_t)\vec{W}_0 \qquad (30)$$

Поле $\vec{W}_t$ определяется формулой (7).

Матрица R в (25) может быть представлена в форме:

$$R = \frac{1}{2ik\chi(k+\chi)}\left[B_0^2 h^2 - (p_{10} + p_{20})E + \Delta E\right]B \tag{31}$$

где

$$p_{10} = b_{12}b_{21};\ p_{20} = b_{78}b_{87}$$

$$\Delta = \sqrt{(p_{10} - p_{20})^2 - 4i\omega b_{17}^2 b_{21} b_{78}} \tag{32}$$

Таким образом, в данной статье приведена матричная формулировка задач отражения – преломления термоупругих волн на границах раздела различных сред.

СПИСОК ЛИТЕРАТУРЫ

1 **Тлеукенов, С.К., Ильясов, М.Н., Досумбеков, К.Р.** О матричной формулировке задачи отражения и преломления термоупругих волн // Материалы международной научной конференции «Вторые Ержановские чтения», г. Актобе, 2007 г.

2 **Тлеукенов, С.К., Досумбеков, К.Р., Сейтханова, А.К.** О коэффициентах отражения и преломления упругих и термоупругих волн // Материалы международной научной конференции «Вторые Ержановские чтения», г. Актобе, 2007 г.

3 **Сейтханова, А.К.** О задаче отражения – преломления упругой волны на границе термоупругого полупространства // Вестник ПГУ. Серия Физико-математическая, № 4, Павлодар, НИЦ ПГУ им. С. Торайгырова, 2010 г.

4. **Тлеукенов, С.К.** Метод матрицанта. – Павлодар: НИЦ ПГУ им. С. Торайгырова, 2004. – 148 с.

Павлодарский государственный университет
имени С. Торайгырова, Павлодар.
Материал поступил в редакцию 05.06.13.

Н. А. Испулов, А. К. Сейтханова

Термосерпімді толқындардың шағылу-сыну есептердің матрицалық формулировкасы

С. Торайғыров атындағы Павлодар
мемлекеттік университеті, Павлодар қ.
Материал 05.06.13 редакцияға түсті.

N. A. Ispulov, A. K. Seitkhanova

The matrix formulation of problems of reflection-refraction of thermoelastic waves

Pavlodar State University named after S. Toraigyrov, Pavlodar.
Material received on 05.06.13.

Термомеханикалық эффектімен болатын серпімді орталарда толқындық процестердің заңдылықтарды зерттеу актуалдығы, геофизика, сейсмология, композиттік материалдардың механикасының теориялық және қолданбалы есептерді шешуінде қажеттілігімен байланысты. Байланысқан қозғалыс теңдеулері мен жылуөткізгіштік теңдеулері физика–механикалық параметрлердің курделігі мен көп болуымен ерекшеленеді. Осыған байланысты деформацияланатын қатты дене механикасының – термосерпімділік деген тарауы қарқынды дамып келеді. Осы бағыттың аясында анизотропты орталардың кейбір физика–механикалық қасиеттерін қолдана отырып, байланысқан жылулық және механикалық өрістер зерттеледі.

Берілген мақалада әртүрлі орталардың шекаралардың бөлімдеріндегі термосерпімді толқындардың шағылу-сыну есептердің матрицалық формулировкасы келтірілген.

The urgency of research of laws of wave processes in elastic environments with thermo mechanical effect is connected with necessity of the decision of theoretical and applied problems of geophysics, seismology, mechanics of composite materials etc. Connected equations of movement and the heat conductivity equation differ complexity and an abundance of physical–mechanical parameters. In this connection the section of mechanics of a deformable firm body, - thermo elasticity intensively develops. Within the limits of this direction, leaning against use of certain physical–mechanical properties anisotropic environments, the connected thermal and mechanical fields are studied.

In this article the matrix formulation of problems of reflection – refraction of thermoelastic waves is given in demarcations of various environments.

ӘОЖ 517:97

М. Мұхтаров, Г. Мұрат

САТЫЛЫ ОЙЫННЫҢ ШЕШІМІН ИНТЕГРАЛДЫ-ДИФФЕРЕНЦИАЛДЫҚ ТЕҢДЕУЛЕР ЖҮЙЕСІ АРҚЫЛЫ АНЫҚТАУ ТУРАЛЫ ЕСЕП

Шешімі интегралды-дифференциалдық теңдеулер жүйесі арқылы анықталатын сатылы ойын қарастырылады.

Қарастырылып отырған сатылы ойында басқарылатын динамикалық жүйе дифференциалдық теңдеу түрінде берілген:

$$x = A\ t\ x + B\ t\ u + C(t)v \qquad (1)$$

Мұндағы $x = x\ t\ \in R^n$ - фазалық вектор, $u = u(t)$ және $v = v(t)$ ойыншылардың басқару функциялары, ал $A(t)$, $\mathrm{B}(t)$ және $\mathrm{C}\ t$ барлық $t \in\ t_0, t_1$ бойынша үзіліссіз матрицалар болсын.

Басқару сапасын бағалайтын функционалдар

$$\mathcal{J}_1\ \mathrm{u,v} = \frac{1}{2} \int_{t_0}^{t_1} u^T \mathrm{F(t)u} + 2u^T \mathrm{G(t)v}\ dt \qquad (2)$$

және

$$\mathcal{J}_2\ \mathrm{u,v} = \frac{1}{2} \int_{t_0}^{t_1} x^T \mathrm{W(t)x} + v^T \mathrm{P(t)v} + 2u^T \mathrm{Q(t)v} + u^T \mathrm{R(t)u}\ dt \qquad (3)$$

түрінде берілген

Есептің қойылуы бойынша (1) жүйені берілген бастапқы $x\ t_0\ = x_0$ күйінен соңғы $x\ t_1\ = x_1$ күйіне көшіре алатын және тиісінше (2) және (3) функционалдарын минимумдайтын Штакельберг мағынасында тиімді $u^0\ t$ және $v^0\ t$ басқару функцияларын құру керек.

Мұндай функциялар біртіндеп екі есептің шешімін табу арқылы анықталады:

1^0 Ойын сатысының жоғарғы деңгейіндегі ойыншының $t \in\ t_0, t_1$ бойынша үзіліссіз $v(t)$ басқару функциясы қандай болса да, төменгі деңгейдегі ойыншының (1) жүйені алғашқы $x\ t_0\ = x_0$ күйінен $x\ t_1\ = x_1$ күйіне көшіре алатын және (2) функционалды

минимумдайтын $t \in t_0, t_1$ бойынша үзіліссіз $u^0\ t, v\cdot$ тиімді басқару функциясын табу керек, яғни

$$\mathcal{J}_1\ u^0\cdot, v\cdot\ , v\cdot\ = \min_u \mathcal{J}_1\ u\cdot, v\cdot \qquad (4)$$

2^0 Айталық, $u^0\ t, v\cdot$ функциясы бірінші есептің шешімі болсын. Онда жоғарғы деңгейдегі ойыншының $u = u^0\ t, v\cdot$ болғанда (3) функционалды минимумдайтын $t \in t_0, t_1$ бойынша үзіліссіз $v^0(t)$ тиімді басқару функциясын табу керек, яғни

$$\mathcal{J}_2\ u^0\cdot, v^0\cdot\ , v^0\cdot\ = \min_v \mathcal{J}_2\ u^0\cdot, v\cdot\ , v\cdot \qquad (5)$$

Осылай анықталған $u^0\ t\ = u^0\ t, v^0\cdot$ және $v^0\ t$ басқарушы функциялар жұбын (1)-(3) сатылы ойынның Штакельберг бойынша тиімді шешімі деп атаймыз.

Қойылған есептің шешімін табу үшін вариациялық әдістер қолданылады. Бірінші есептің шешімі оны изопериметрлік есепке келтіру арқылы анықталады. Осы амалдар нәтижесінде алынған шешім келесі түрде жазылады:

$$u^0\ t, v\cdot\ = -F^{-1}\ G\ t\ v\ t\ + \int_{t_1} +H_1{}^0\ t_1, t\ \mathrm{D}\ \int_{t_0} S\ \tau\ v\ \tau\ d\tau - d^{\ 0} \qquad (6)$$

Мұндағы белгілеулер:

$$S\ t\ = H_2{}^0\ t_1, t\ - H_1{}^0\ t_1, t\ F^{-1}G\ t\ ,$$

$$\mathrm{D} = \int_{t_0}^{t_1} H_1{}^0\ t_1, \tau\ F^{-1}\ \tau\ H_1{}^{0\ T}\ t_1, \tau\ d\tau \Big)^{-1}$$

$$d^{\ 0}\ = x_1 - X(t_1, t_0)x_0$$

$$H_1{}^0\ t, \tau\ = X(t, \tau)B\ \tau\ , H_2{}^0\ t, \tau\ = X(t, \tau)C\ \tau$$

$X(t, \tau)$ – матрицасы $x = A\ t\ x, X\ t, t\ = E$, Е-бірлік матрица – біртекті жүйенің іргелі матрицасы.

Екінші есептің шешімін іздеу амалында сәйкес функциялар мен функционалды вариациялау арқылы келесі интегралды-дифференциалдық теңдеулер жүйесіне келеміз:

$$x = Ax + S_2\ t\ v^0\ t\ - \Lambda\ t \int_{t_0}^{t_1} S\ \tau\ v^0\ t\ d\tau - d^{\,0}$$

$$x\ t_0\ = x_0,\ x\ t_1\ = x_1$$

$$\psi = -A^T\psi - W\ t\ x,$$

$$v^0\ t\ + \int_{t_0}^{t_1} K\ t,\tau\ v^0\ \tau\ d\tau = g\ t\ - L^{-1}S_2^T\ t\ \psi\ t\ +$$

$$+L^{-1}\ t\ S^T\ t \int_{t_0}^{t_1} \Lambda^T\ \tau\ \psi\ \tau\ d\tau \qquad 7$$

Мұндағы белгілеулер:

$S_2\ t\ = C\ t\ - B\ t\ F^{-1}\ t\ G\ t\ ,$

$$\Lambda\ t\ = B\ t\ F^{-1}\ t\ H_1{}^{0\ T}\ t_1, t\ \mathrm{D}$$

$$L\ t\ = P\ t\ - G^T\ t\ F^{-1}\ t\ Q\ t\ - Q^T\ t\ F^{-1}\ t\ G\ t\ +$$
$$+G^T\ t\ F^{-1}\ t\ R\ t\ F^{-1}\ t\ G\ t\ ,$$

$$M\ t\ = G^T\ t\ F^{-1}\ t\ R\ t\ - Q^T\ t\ F^{-1}\ t\ H_1{}^{0\ T}\ t_1, t\ D,$$

$$N\ t\ = D^T H_1{}^0\ t_1, t\ F^{-1}\ t\ R\ t\ F^{-1}\ t\ H_1{}^{0\ T}\ t_1, t\ D$$

Тағы да

$$K\ t,\tau\ = L^{-1}\ t\ \ M\ t\ + S^T\ t \int_{t_0}^{t_1} N\ \theta\ d\theta\ S\ t\ + L^{-1}\ t\ S^T\ t\ M^T\ \tau$$

$$g\ t\ = L^{-1}\ t\ \ M\ t\ + S^T\ t \int_{t_0}^{t_1} N\ \theta\ d\theta\ d^{\,0}$$

Бұл жүйедегі $K\ t,\tau$, $S\ t$, $\Lambda\ t$ ядролары интегралдық теңдеулер теориясында қойылған шарттарды қанағаттандырады.

Соңғы (7)-ші интегралды-дифференциалдық теңдеулер жүйесінен анықталған $v^0\ t$ функциясын (6) теңдікке қойып $u^0\ t$ басқару функциясын табамыз.

Осылай анықталған $u^0\ t$ және $v^0\ t$ басқарушы функциялары (1)-(3) сатылы ойынның тиімді шешімі болып табылады.

Осы алынған нәтижелерді пайдаланып келесі басқару есебінің шешімін табайық.

Есеп. Сызықты жүйе

$$\begin{aligned} x_1 &= x_2 \\ x_2 &= u + v \end{aligned} \tag{8}$$

түрінде берілген болсын.

Минимумдалатын функционалдар келесі түрде берілген:

$$J_1 = \frac{1}{2}\int_0^1 u^2 dt, \tag{9}$$

$$J_2 = \frac{1}{2}\int_0^1 x^2 + u^2 + v^2 \, dt \tag{10}$$

Бұл есепте бірінші жүйені берілген $x\ 0\ =\ 1{,}0$ алғашқы күйінен соңғы $x\ 1\ =\ 0{,}0$ күйіне көшіретін және 9 , 10 функционалдарды минимумдайтын $u^0\ t\ , v^0\ t$ тиімді басқару функцияларын табу керек. Есептің шешімін іздеуден бұрын алдын-ала қажетті есептеулерді жүргізейік. Бұл жағдайда:

$$A = \begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}, B = C = \begin{matrix} 0 \\ 1 \end{matrix}, F = 1, G = Q = 0, P = R = 1,$$

$$W = \begin{matrix} 0 & 0 \\ 0 & 1 \end{matrix}, X\ t, \tau\ = \begin{matrix} 1 & t-\tau \\ 0 & 1 \end{matrix}$$

$$d^{\,0} = \begin{matrix} 1 \\ 0 \end{matrix}, \quad H_1^{\,0}\ t_1, \tau\ = H_2^{\,0}\ t_1, \tau\ = \begin{matrix} 1-t \\ 1 \end{matrix},$$

$$D = \int_0^1 N\ \theta\ d\theta = 2\begin{matrix} 6 & -3 \\ -3 & 2 \end{matrix}, S_2 = \begin{matrix} 0 \\ 1 \end{matrix}, S\ t\ = \begin{matrix} 1-t \\ 1 \end{matrix},$$

$$\Lambda\ t\ = 2\begin{matrix} 0 & 0 \\ 3-6t & 3t-1 \end{matrix}, \quad K\ t, \tau\ = 2(3-6t\ \ 3t-1)\begin{matrix} 1-\tau \\ 1 \end{matrix}$$

$$M = 0, \quad L = 1, g\ t\ = 12t - 6$$

Осы теңдіктерді (7) интегралды-дифференциалдық теңдеулер жүйесіне қойып мынадай жүйе аламыз:

$$x_1 = x_2$$

$$x_2 = v^0\ t\ -2\ 3-6t \int_0^1 1-\tau\ v^0\ \tau\ d\tau - \int_0^1 -2\ 3t-1\ v^0\ \tau\ d\tau + 12t - 6, \qquad (11)$$

$$x_1\ 0\ = 1,\ x_2\ 0\ = 0, \qquad x_1\ 1\ = x_2\ 1\ = 0$$

$$\psi_1 = 0$$

$$\psi_2 = -x_2 - \psi_1$$

$$v^0\ t\ +\ 6-12t \int_0^1 1-\tau\ v^0\ \tau\ d\tau + \ 6t-2 \int_0^1 v^0\ \tau\ \mathrm{d}\tau =$$

$$= 12\mathrm{t} - 6 - \psi_2\ t\ +\ 1-t \int_0^1 6-12\tau\ \psi_2\ \tau\ d\tau +$$

$$+ \int_0^1 6\tau - 2\ \psi_2\ \tau\ d\tau$$

Мұндағы соңғы интегралдық теңдеудің шешімі мына түрде алынады:

$$v^0\ t\ = 6t - 3 - \psi_2 + \ 12t-6 \int_0^1 \tau\psi_2\ \tau\ d\tau + \int_0^1 4-6t\ \psi_2\ \tau\ d\tau \qquad 12$$

Осыны (11) жүйенің екінші теңдеуіне қоямыз да, келесі жүйені аламыз:

$$x_1 = x_2$$

$$x_2 = 12t - 6 - \psi_2 + \ 12t-6 \int_0^1 \tau\psi_2\ \tau\ d\tau + \ 4-6t \int_0^1 \psi_2\ \tau\ d\tau \qquad (13)$$

$$x_1\ 0\ = 1,\ x_2\ 0\ = 0, \qquad x_1\ 1\ = x_2\ 1\ = 0$$

$$\psi_1 = 0$$

$$\psi_2 = -x_2 - \psi_1$$

Соңғы жүйеден

$$\psi_2 = \psi_2 - 12t + 6 - \int_0^1 (12t - 6)\,\tau\psi_2\,\tau\,d\tau - \int_0^1 (4 - 6t)\,\psi_2\,\tau\,d\tau$$

теңдеуін аламыз. Оның шешімінің түрі:

$$\psi_2\,t = e - 3^{-1}\,e^t - e^{1-t} + 12t - 6 \qquad (14)$$

Осы (14) шешімді (12) –ші өрнекке қойып

$$v^0\,t = e - 3^{-1}\,e^{1-t} - e^t - 6t + 3 \qquad (15)$$

функциясын аламыз.

Енді $u^0\,t$ функциясын есептейміз

$$u^0\,t = \int_0^1 (12t - 6)\,(1 - \tau)\,v^0\,\tau\,d\tau +$$

$$+ \int_0^1 (2 - 6t)\,v^0\,\tau\,d\tau + 12t - 6 = 6t - 3 \qquad (16)$$

Осы түрде анықталған $u^0\,t$, $v^0\,t$ шешімді басқару функцияларының жұбына сәйкес тиімді қозғалыс төменгі түрде алынады:

$$x_1^0 = e - 3^{-1}\,e^{1-t} - e^t + e + 1\,t - 2\,,$$

$$x_2^0 = e - 3^{-1}\,-e^{1-t} - e^t + e + 1 \qquad (17)$$

Бұл өрнектен $x_1^0\,0 = 1,\ x_2^0\,0 = 0, x_1^0\,1 = 0, x_2^0\,1 = 0$ шарттарының орындалатындығына көз жеткізу қиын емес.

ӘДЕБИЕТТЕР ТІЗІМІ

1 **Al'brekht, E. G., Mukhtarov, M. M.** On the Design of Optimal open-loop Controllers in some Quasilinear Hierarchical Games. // Problems of Control and Information Theory. Vol. 14 (4), pp. 247-259 (1985)

2 **Simaan, M., Cruz, J. B.** Additional Aspects of the Stackelberg Strategy in Nonzero-Sum Games. // J. Optim. Theory Appl., Volume 11, No. 6, 1973. – pp. 613-626.

3 **Васильева, А. Б., Тихонов, Н. А.** Интегральные уравнения. – М. : Изд-во Моск. ун-та, 1980. – 156с.

4 **Красовский, Н. Н., Субботин, А. И.** Позиционные дифференциальные игры. – М. : Наука, 1974. - 456с.

5 **Красовский, Н. Н.** Управление динамической системой. – М. : Наука, 1985. – 520с

6 **Эльсгольц, Л. Э.** Дифференциальные уравнения и вариационное исчисление. М. : Наука, 1965. – 424с.

7 **Мұхтаров, М.** Вариациялық есептеу. – Павлодар: Кереку, 2012. – 174 б.

8 **Мұхтаров, М.** Дифференциалдық теңдеулер бойынша дәрістер. – Павлодар: Кереку, 2010. – 394 б.

С. Торайғыров атындағы Павлодар
мемлекеттік университеті, Павлодар қ.
Материал 31.05.13 редакцияға түсті.

М. Мухтаров, Г. Мурат

Задача о нахождении решения иерархической игры с помощью системы интегро-дифференциальных уравнений

Павлодарский государственный университет
имени С. Торайгырова, Павлодар.
Материал поступил в редакцию 31.05.13.

M. Mukhtarov, G. Murat

The problem of finding solutions hierarchical games using a system of integro-differential equations

Pavlodar State University named after S. Toraigyrov, Pavlodar.
Material received on 31.05.13.

Рассматривается иерархическая игра, решение которой определяется с помощью системы интегро-дифференциальных уравнений.

We consider a hierarchical game, the decision of which is determined by a system of integro-differential equations.

УДК 532.546

Р. К. Сагындыкова, У. М. Туганбаев

ИССЛЕДОВАНИЕ ДВУМЕРНОГО УРАВНЕНИЯ ТЕПЛОПРОВОДНОСТИ В ПОЧВОГРУНТАХ

Рассматривается двумерное уравнение теплопроводности, для которого найдены четыре вида автомодельных решений

Известно, что почва представляет собой многофазную капиллярно-пористую структуру, внутри которой осуществляется следующая теплопередача одновременно: в местах непосредственного контакта частиц, излучением от частицы к частице, конвекцией и теплопроводностью в межпоровом пространстве и в результате переноса влаги. Все эти процессы можно свести к четырем типам процессов: кондуктивной теплопроводности, конвекции в порах, излучению в порах, переносу. Распространение и нахождение тепла внутри почвы, где действуют все эти факторы, является трудной проблемой и исключительной сложности. Для этого, необходимо составить для каждого конкретного случая, системы из четырех уравнений. Если рассматривать почву как квазиоднородное тело, параметры теплопереноса учитывают совокупность всех перечисленных факторов, тогда для описания распространения тепла в почве достаточно одного дифференциального уравнения в частных производных второго порядка параболического типа, но с эквивалентными коэффициентами. Для решения этого подхода, необходимо решить уравнение теплопроводности при различных краевых условиях, и второе, располагать данными о теплофизических характеристиках в зависимости от внутренних особенностей почвенного материала, т.е., имеется в виду: от плотности, дисперсности, влажности, химико-минералогического состава и т.д. Таким образом, для анализа и нахождения температурного поля можно отказаться от системы уравнений кондуктивной, радиационной и массообменной проводимости, а ограничиться лишь одним уравнением теплопроводности с осложненной за счет всех вышеуказанных факторов коэффициентов теплопереноса [1].

$$C(x,y,t)\frac{\partial T}{\partial t}=\frac{\partial}{\partial x}\left[\lambda(x,y,t)\frac{dT}{dx^2}\right]+\frac{d}{dy}\left[\lambda(x,y,t)\frac{dT}{dy}\right] \quad (1)$$

Из сказанного следует, что термические характеристики: λ – коэффициент теплопроводности, С – коэффициент объемной теплоемкости, имеют решающее значение при изучении, оценке и регулирование теплового режима в почве. Знание вышеуказанного комплекса характеристик крайне необходимо при решении большого количества важных агротехнических задач. Эти характеристики определяют собой распределение температуры в почве, ход этой температуры на различные глубины почвы по времени, количества тепла, получаемого поверхностью почвы благодаря солнечной радиации, причем это тепло частично проникает в пахотный слой почвы и аккумулируется в ней. Весьма важно знать, какая ожидается температура почвы через определенное время, какова тенденция этой температуры, как она будет меняться в течении суток, сезона и всего года. Важно также знать содержание тепла в почве и какие меры нужно и можно предпринять для того, чтобы уменьшить или увеличить количество тепла в ней. Проблема теплопереноса в почве, за последние годы, превратилось в развивающую отрасль так как ее теоретические, методические и экспериментальные достижения проникли в самые разнообразные области агропромышленного комплекса и ее научных исследований [1]. Основной нашей задачей является определение аналитических частных решений уравнения теплопроводности (1) с начально-краевыми условиями:

$T(x,y,0)=\varphi_1(x,y)$ - распределение начального условия (2)

$T(0.0,t)=\varphi_2(t)$ - на поверхности (2а)

$T(H_0,Y_0,t)=\varphi_3(t)$, $T(X_0,H_1,t)=\varphi_4(t)$ – распределение температуры на глубине $x=H_0$, $y=H_1$ (2б)

Для определения решений нелинейного уравнения (1), поступим следующим образом. Разлагая коэффициенты теплопроводности и теплоемкости на поверхности почвы в нулевом приближении имеем $\lambda(x,y,t)\approx\lambda_0$, $C(x,y,t)\approx C_0$. В этом случае, уравнение (1) запишется $(\tau=\lambda_0 t/c_0)$ как: $T_\tau=T_{xx}+T_{yy}$ (3)

которое является уравнением наших последующих исследований.

I. Ищем решение (3) в форме $T(x,y,\tau)=\tau^m f(\xi)$, $\xi=-\frac{1}{8}\frac{(x+y)^2}{\tau}$ (4)

Определяя частные производные: $T_\tau=\tau^{m-1}[mf-\xi f']$,

$T_{xx}=\tau^{m-1}\left[-\frac{1}{2}\xi f''-\frac{1}{4}f'\right]$, $T_{yy}=\tau^{m-1}\left[-\frac{1}{2}\xi f''-\frac{1}{4}f'\right]$ и подставляя в рассматриваемое уравнение (3), получим

$$\xi f''+\left[\frac{1}{2}-\xi\right]f'+mf=0, \qquad (5)$$

Вырожденное гипергеометрическое уравнение Гаусса, которое имеет два вида класса частных решений [2]

$$f(\xi)=C_1F(-m;\frac{1}{2};\xi)+C_2\xi^{1/2}F(-m+\frac{1}{2};\frac{3}{2};\xi) \qquad (6)$$

где $F(\xi)=1+\frac{a}{b\cdot 1!}\xi+\frac{a(a+1)}{b(b+1)2!}\xi^2+...+\frac{(a+R-1)}{(b+R-1)\cdot R!}\xi^R+...$ – функция Похгаммера или вырожденная гипергеометрическая функция, и представленная с помощью ряда, сходящегося при всех значениях ξ.

При любых преобразованиях Куммера, можно получить другие классы частных решений исследуемого уравнения [2].

II. Если же искать решение уравнения(3) в другом виде.

$$T(x,y,\tau)=(x+y)^n\cdot f(\eta), \qquad \eta=\frac{b\tau}{(x+y)^2} \qquad (7)$$

при этом $\eta_\tau=\frac{b}{(x+y)^2}$, $\eta_x=\frac{2b\tau}{(x+y)^3}$, $\eta_Y=\frac{2b\tau}{(x+y)^3}$, а

$T_\tau=(x+y)^{n-2}\cdot bf'$, $T_{xx}=(x+y)^{n-2}\left[4\eta^2f''+2(3-2n)\eta f'+n(n-1)f\right]$,

$T_{yy}=(x+y)^{n-2}\left[4\eta^2f''+2(3-2n)\eta f'+n(n-1)f\right]$

Подставляя их в уравнение(3), после некоторых математических действий, получим

$$\eta^2f''+\left[\frac{3-2n}{2}\eta-\frac{b}{8}\right]f'+\frac{n(n-1)}{4}f=0 \qquad (8)$$

A. Для решения уравнения (8) поступим следующим образом [2]

Пусть $f(\eta(=\exp(\eta_1)\cdot\eta_1^2\cdot f_1(\eta_1)$, где $\eta_1=\eta^{-1}$, (9)

v-корень уравнения $v^2+(1-a)v+c=0$, $a=\frac{3-2n}{2}$, $c=\frac{n(n-1)}{4}$, получаем следующее уравнение

$$\eta f_1''(\eta)+\left[\eta+\frac{4n+1}{2}f_1'(\eta)+\frac{3n+1}{2}f_1(\eta)\right]=0\,, \qquad (10а)$$

$$\eta f_1''(\eta)+\left[\eta+\frac{4n-1}{2}f_1'(\eta)+\frac{3n}{2}f_1(\eta)\right]=0, \qquad (10б)$$

где $v_1=\frac{n}{2}$, $v_2=\frac{n-1}{2}$, а решениями уравнения при b=1, $a-2=C=-\frac{2n+1}{2}$

будет $f(\eta)=\eta^{(2n+1)/2}\cdot\exp(1/\eta)\left[c_1+c_2\int\eta^{(2n+5)/2}\cdot\exp(-1/\eta)d\eta\right]$ (11)

Б. Если же искать решения уравнения (8) в виде алгебраического полинома второй степени $f(\eta)=B_0\eta^2+B_1\eta+B_2$, (12)

то подставляя его, вместе с его производными в уравнение (8) получим следующую систему

$$\begin{aligned}&1.\ B_0(n^2-9n+20)=0\,,\\ &2.\ -bB_0+B_1(n^2-5n+6)=0\,,\\ &3.\ -bB_1+2n(n-1)B_2=0\end{aligned} \qquad (13)$$

Разрешая эту систему получим два решения при n=4 и n=5

1. $f(\eta)=B_0\eta^2+\frac{bB_0}{2}\eta+\frac{b^2B_0}{48}$, 2. $f(\eta)=B_0\eta^2+\frac{bB_0}{6}\eta+\frac{b^2B_0}{240}$.

Таким образом, искомая функция запишется

$$T(x,y,\tau)=(x+y)^4\cdot B_0\left[\eta^2+\frac{b}{2}\eta+\frac{b^2}{48}\right],\ \text{при}\quad n=4, \qquad (14а)$$

$$T(x,y,\tau)=(x+y)^5\cdot B_0\left[\eta^2+\frac{b}{6}\eta+\frac{b^2}{240}\right],\ \text{при}\quad n=5 \qquad (14б)$$

где величины b и B_0 -произвольны.

В.Если же искать решение уравнения (8) в виде алгебраического полинома третьей степени $f(\eta)=B_0\eta^3+B_1\eta^2+B_2\eta+B_3$ (15)

то проделав те же выкладки, что и выше, получим систему

$$\begin{aligned}&1.\ B_0(n^2-13n+42)=0, \qquad 2.\ -3bB_0+2B_1(n^2-9n+20)=0\\ &3.\ -bB_1+B_2(n^2-5n+6)=0, \qquad 4.\ -bB_2+2n(n-1)B_3=0.\end{aligned} \qquad (16)$$

Из первого уравнения находим корни: $n_1=6$, $n_2=7$, B_0 и b-произвольны, тогда: $f(\eta)=B_0\eta^3+\frac{3bB_0}{4}\eta^2+\frac{b^2B_0}{16}\eta+\frac{b^3B_0}{960}$, при n=6, (17а)

$$f(\eta)=B_0\eta^3+\frac{bB_0}{4}\eta^2+\frac{b^2B_0}{80}\eta+\frac{b^3B_0}{6720},\ \text{при}\quad n=7, \qquad (17б)$$

а искомая функция, с учетом предполагаемого решения (7) окончательно запишется

$$T(x,y,\tau)=(x+y)^6\cdot B_0\left[\eta^3+\frac{3b}{4}\eta^2+\frac{b^2}{16}\eta+\frac{b^3}{960}\right], \qquad (18а)$$

$$T(x,y,\tau)=(x+y)^7\cdot B_0\left[\eta^3+\frac{b}{4}\eta^2+\frac{b^2}{80}\eta+\frac{b^3}{6720}\right]. \qquad (18б).$$

Г. И наконец, рассмотрим решение уравнения (8) в виде

$$f(\eta)=B_0\eta^4+B_1\eta^3+B_2\eta^2+B_3\eta+B^4 \qquad (19)$$

в результате получим систему из пяти уравнений

1. $B_0(n^2-17n+72)=0$,
2. $-2bB_0+B_1(n^2-13n+42)=0$,
3. $-3bB_1+2B_2(n^2-9n+20)=0$,
4. $-bB_2+B_3(n^2-5n+6)=0$,
5. $-bB_3+2n(n-1)B_4=0$ (20)

Из первого уравнения находим корни : $n_1=8, n_2=9$. B_0 и b-произвольные, а решение (19) запишется как

$$f(\eta)=B_0\eta^4+\frac{bB_0}{105}\eta^3+\frac{b^2B_0}{840}\eta^2+\frac{b^3B_0}{25200}\eta+\frac{b^4}{282240}, \text{ при } n=8, \qquad (21а)$$

$$f(\eta)=B_0\eta^4+\frac{bB_0}{120}\eta^3+\frac{b^2B_0}{1600}\eta^2+\frac{b^3B_0}{67200}\eta+\frac{b^4}{967680}, \text{ при } n=9 \qquad (21б)$$

В этом случае искомые функции примут форму

$$T(x,y,\tau)=(x+y)^8\cdot B_0\left[\eta^4+\frac{b}{105}\eta^3+\frac{b^2}{840}\eta^2+\frac{b^3}{25200}\eta+\frac{b^4}{2822400}\right], \qquad (22а)$$

$$T(x,y,\tau)=(x+y)^9\cdot B_0\left[\eta^4+\frac{b}{120}\eta^3+\frac{b^2}{1600}\eta^2+\frac{b^3}{67200}\eta+\frac{b^4}{9676800}\right], \qquad (22б)$$

Анализ, полученных решений вида (7), показывает, что при увеличе-нии параметра n, степень алгебраического полинома также увеличивается. Поэтому можем записать решение в общем виде уравнения (3), записанное в форме (7) как

$$T(x,y,\tau)=(x+y)^{2n}\cdot\left[B_0\eta^n+B_1\eta^{n-1}+\ldots+B_{2n-4}\eta+B_{2n-3}\right], \text{ при } n=2n \qquad (23а)$$

$$T(x,y,\tau)=(x+y)^{2n+1}\cdot\left[B'_0\eta^n+B'_1\eta^{n-1}+\ldots+B'_{2n-4}\eta+B'_{2n-3}\right], \text{ при } n=2n+1 \qquad (23б).$$

III. Предположим, что решение уравнения (3) можно искать в форме

$$T(x,y,\tau)=\tau^m\cdot(x+y)^n\cdot f(\xi),\qquad \xi=b\frac{(x+y)^2}{\tau} \tag{24}$$

при этом $\xi_\tau=-\frac{\xi}{\tau}$, $\xi_x=\frac{2\xi}{(x+y)}$, $\xi_y=\frac{2\xi}{(x+y)}$.

Определяя частные производные T_τ, T_{xx}, T_{yy}, подставляя в (3) получим следующее уравнение

$$\xi^2 f''(\xi)+\left[\frac{1}{8b}\xi^2+\frac{2n+1}{2}\xi\right]f'(\xi)+\left[\frac{n(n-1)}{4}-\frac{m}{8b}\xi\right]f(\xi)=0 \tag{25}$$

Это уравнение при $n=1$, $b=-\frac{1}{8}$ запишется в виде вырожденного гипер-геометрического уравнения Гаусса

$$\xi f''(\xi)+\left[\frac{3}{2}-\xi\right]f'(\xi)+mf(\xi)=0 \tag{26}$$

которое имеет решения

$$f(\xi)=c_1F\left(-m,\frac{3}{2},\xi\right)+c_2\xi^{1/2}F\left(-m-\frac{1}{2},\frac{1}{2},\xi\right) \tag{27}$$

Эти решения, при следующих функциональных преобразованиях [2]

$$1.\ F(a,b,\xi)=e^{\xi}\cdot F(b-a,b,\xi),\quad 2.\ F(a,b,\xi)-bF'(a,b,\xi)=a(a-1)/b(b+1)\xi F(a+1,b+2,\xi)$$

$$3.\ F(a,b,\xi)=(a/b)\cdot F(a+1,b+1,\xi)\ 4.\ F(a,b,\xi)-F'(a,b,\xi)=b-a/b\cdot F(a,b+1,\xi), \tag{28}$$

могут иметь другие классы частных решений.

А. Теперь для нахождения решения уравнения (25),будем искать его в форме полинома

$$f(\xi)=B_0\xi^2+B_1\xi+B_2 \tag{29}$$

и получим систему

$$\begin{aligned}
&1.\ B_0(2-m)=0,\\
&2.\ 2bB_0(n^2+7n+4)+B_1(1-m)=0,\\
&3.\ 2bB_1(n^2+3n+2)-mB_2=0,\\
&4.\ 2n(n-1)bB_2=0
\end{aligned} \tag{30}$$

Разрешая, эту систему получим $B_2=0$, $m=2$, B_0-произвол, $B_1=2b(n^2+7n+4)B_0)$, тогда искомая функция запишется $f(\xi)=B_0\xi^2+2b(n^2+7n+4)B_0\xi$, а с учетом (24), функция теплопроводности примет вид $T(x,y,\tau)=\tau^2(x+y)^n(B_0\xi^2+2b(n^2+7n+4)B_0\xi)$ (31)

или в искомых переменных

$$T(x,y,\tau)=(x+y)^{n+2}b^2B_0\left[(x+y)^2+2(n^2+7n+4)\tau\right] \qquad (32)$$

Б. Предположим, что решение (25) можно найти в форме полинома третьей степени $f(\xi)=B_0\xi^3+B_1\xi^2+B_2\xi+B_3$. (33)

в результате которого имеем систему для определения коэффициентов выражения (33).

1. $B_0(3-m)=0$,
2. $2bB_0(n^2+11n+30)=(m-2)B_1$,
3. $2bB_1(n^2+7n+12)=(m-1)B_2$,
4. $2bB_2(n^2+3n+2)=mB_3$,
5. $n(n-1)bB_3=0$ (34)

Так как у нас величины n, m, B_1 пока произвольные, можно рассматриваемую систему решить при их различных значениях

а) При $m=3, n=1$, B_0- произвольном имеем $B_1=84bB_0, B_2=3360b^2B_0$, $B_3=13440b^3B_0$ т. е. функция $f(\xi)$ запишется

$$f(\xi)=B_0\xi^3+84bB_0\xi^2+3360b^2B_0\xi+13440b^3B_0, \qquad (35)$$

а сама функция теплопроводности, как

$$T(x,y,\tau)=\tau^3(x+y)\left(B_0\xi^3+84bB_0\xi^2+3360b^2B_0\xi+13440b^3B_0\right). \qquad (36)$$

б) Систему (34) решим следующим образом. Из уравнений (1,4,5) системы (34).имеем $m=0$, $B_3=0$, $n_1=-2, n_2=-1, B_2$-произвол.

Тогда разрешая всю систему уравнений (34).получим

$$f_1(\xi)=B_2\xi\left(1+\frac{1}{2b}\xi+\frac{1}{144b^2}\xi^2\right) \qquad \text{при} \quad n=-2 \qquad (36а)$$

$$f_2(\xi)=B_2\xi\left(1+\frac{1}{6b}\xi+\frac{1}{240b^2}\xi^2\right) \qquad \text{при} \quad n=-1 \qquad (36б)$$

а сама искомая функция теплопроводности, запишется

$$T_1(x,y,\tau)=\frac{\tau^2}{(x+y)^2}bB_2\left[(x+y)^2+\frac{1}{2}(x+y)\cdot\tau+\frac{1}{144}\tau^2\right] \qquad (37а)$$

$$T_2(x,y,\tau)=\frac{\tau}{(x+y)}bB_2\left[(x+y)^2+\frac{1}{6}(x+y)\cdot\tau+\frac{1}{240}\tau^2\right] \qquad (37б)$$

В. И последнее, предположим, что существует решение уравнения (25) в виде полинома $f(\xi)=B_0\xi^4+B_1\xi^3+B_2\xi^2+B_3\xi+B_4$ (38)

Определяя также производные 1-го и 2-го порядка, подставляя в рассматриваемое уравнение, получим систему вида

1. $B_0(4-m)=0$, 2. $2bB_1(n^2+15n+56)=(m-3)B_1$, 3. $2bB_2(n^2+11n+30)=(m-2)B_2$,

4. $2bB_2(n^2+7n+12)=(m-1)B_3$, 5. $2bB_3(n^2+3n+2)=mB_4$, 6. $n(n-1)bB_4=0$.

а). Здесь видно, что при $m=4, n=1$, B_0-произвольном, имеем

$$f(\xi)=B_0(\xi^4+144b\xi^3+6048b^2\xi^2+80640b^3\xi+241920b^4), \quad (40)$$

при этом функция теплопроводности примет вид

$$T(x,y,\tau)=\tau^4(x+y)B_0(\xi^4+144b\xi^3+6048b^2\xi^2+80640b^3\xi+241920b^4) \quad (41а)$$

или $$T(x,y,\tau)=A_0\tau^4(x+y)^{-7}\left[(x+y)^8+\frac{(x+y)^6}{3}\tau+\frac{(x+y)^4}{40}\tau^2+\frac{57(x+y)^2}{120960}\tau^3+\frac{\tau^4}{241920}\right] \quad (41б)$$

б) Систему уравнений (39), решим так: Пусть $m=4, B_4=0, B_0$ - произвольная, $n_1=-2, n_2=-1$.Тогда коэффициенты B_1, B_2 выражаются через B_3 которая также произвольна, т. е. имеем

$$f_1(\xi)=B_3\xi\left(1+\frac{3}{4b}\xi+\frac{1}{16b^2}\xi^2+\frac{1}{960b^3}\xi^3\right) \text{ при} \quad (42а)$$

$$f_2(\xi)=B_3\xi\left(1+\frac{1}{2b}\xi+\frac{1}{40b^2}\xi^2+\frac{1}{3360b^3}\xi^3\right) \text{ при} \quad (42б)$$

А в первоначальных переменных искомая функция теплопроводности запишется

$$T_1(x,y,\tau)=A_3\tau^5(x+y)^{-10}\left[(x+y)^6+\frac{3(x+y)^4}{4}\tau+\frac{(x+y)^2}{16}\tau^2++\frac{\tau^3}{960}\right] \text{ при } n=-2 \quad (43а)$$

Таким образом, нами исследовано двумерное уравнение теплопроводности в различных автомодельных формах в различных алгебраических полиномах. Здесь прослеживается закономерность получения определенных решений. Произвольные постоянные полученных решений определяются из явного задания начально-краевых условий рассматриваемой задачи.

СПИСОК ЛИТЕРАТУРЫ

1 **Чудновский, А. Ф.** Теплообмен в дисперсных средах. – Л. : Гостехиздат, 1954. – 444 с.

2 **Камке, Э.** Справочник по обыкновенным дифференциальным уравнениям. – М. : Наука, 1976. – 576 с.

Кыргызский национальный аграрный университет
имени К. И. Скрябина, г. Бишкек, Кыргызская Республика.
Материал поступил в редакцию 04.09.13.

Р. К. Сагындыкова, У. М. Туганбаев

Жерқыртысындағы жылулық өткізгіштіктің екі өлшемді теңдеудің зерттеуі

К. И. Скрябин атындағы Қырғыз ұлттық аграрлық университеті
Бишкек қ., Қырғыз Республикасы.
Материал 04.09.13 редакцияға түсті.

R. K. Sagyndykova, U. M. Tuganbaev

Research of the two-dimensional equation of heat conductivity in soil.

National Agrarian University named after K. I. Skryabin,
Bishkek, Kyrgyzstan.
Material received on 04.09.13.

Жылулық өткізгіштіктің екі өлшемді теңдеу үшін автосулбілі шешімдерінің төрт түрлері табылытыны қаралды.

The two-dimensional equation of heat conductivity for which is considered, four kinds of automodeling decisions are found.

UDC 517.9

M. M. Sarsengeldin, G. Kospanova

ANALYTICAL SOLUTION OF THE FIRST TYPE BOUNDARY-VALUE PROBLEM FOR THE HEAT EQUATION BY IEF METHOD

Analytical solution of the first type boundary-value problem is found using Integral Error Functions and their properties or by IEF method, which enables to solve analytically wide range of heat equations with moving boundaries, which degenerate into a point at the initial time.

Key words: *Integral Error Functions, IEF method*

Abbreviations: *IEF-Integral Error Function*

Introduction

Auto-model case when the boundary $\alpha(t)$ is moving according to the law $\alpha(t) = c\sqrt{t}$ is considered in [3] where analytical solution is found.

Development of analytical methods of solution of free boundary problems is very important for analysis of dynamics of phenomena of heat and mass transfer with phase transformation.

Solution of the Heat Equation

$$\frac{\partial u}{\partial t} = a^2 \frac{\partial^2 u}{\partial x^2} \tag{1}$$

can be represented in the following form

$$u_n \ \pm x, t \ = t^{\frac{n}{2}} i^n erfc\left(\frac{\pm x}{2a\sqrt{t}}\right) \tag{2}$$

where

$$erfcx = 1 - erfx, \qquad i^n erfcx = \int_x^\infty i^{n-1} erfcv\,dv, \quad n=1,2,\ldots$$

$$i^0 erfcx \equiv erfcx = \frac{2}{\sqrt{\pi}} \int_x^\infty \exp(-v^2)dv \tag{3}$$

Using superposition principle solution (1) can be written in the form of series of (2)

$$u\ x,t \ = \ \sum_{n=0}^{k} A_n u_n \ x,t \ + B_n u_n \ -x,t \ , \tag{4}$$

where coefficients A_n, B_n have to be determined.

Finally solution of the heat equation (1) can be represented in the following form

$$u\ x,t\ =\ \sum_{n=0}^{\gamma}\ \bar{t}^{\ n}\ A_n i^n erfc\frac{x}{2a\ \bar{t}} + B_n i^n erfc\frac{-x}{2a\ \bar{t}} \tag{5}$$

Problem statement.

It is required to find solution of the heat equation

$$\frac{\partial u}{\partial t} = a^2 \frac{\partial^2 u}{\partial x^2}, \quad \beta\sqrt{t} < x < \alpha\sqrt{t}\ , \quad t > 0 \tag{6}$$

Subject to

I.C: $$u(x,0) = 0, \tag{7}$$

B.C: $$u(0,t) = \varphi(t), \tag{8}$$

$$u(l,t) = \phi(t), \tag{9}$$

$$u(0,0) = 0, \tag{10}$$

If functions $\varphi(t), \phi(t)$ are definite functions given in the form $\varphi(t) = \sum_{n=0}^{k} \mu_n t^{\frac{n}{2}}$, $\phi(t) = \sum_{n=0}^{m} \nu_n t^{\frac{n}{2}}$ Then solution can be represented in the form

$$u(x,t) = \sum_{n=0}^{\gamma} \left(\sqrt{t}\right)^n \left[A_n i^n erfc\frac{x}{2a\sqrt{t}} + B_n i^n erfc\frac{-x}{2a\sqrt{t}}\right]$$

Substituting expression into the boundary conditions for $x = \beta\sqrt{t}$

$$u\left(\beta\sqrt{t},t\right) = \sum_{n=0}^{\gamma} \left(\sqrt{t}\right)^n \left[A_n i^n erfc\frac{\beta}{2a} + B_n i^n erfc\frac{-\beta}{2a}\right]$$

or

$$u\left(\beta\sqrt{t},t\right) \equiv \left(\sqrt{t}\right)^0 \left[A_0 i^0 erfc\frac{\beta}{2a} + B_0 i^0 erfc\frac{-\beta}{2a}\right] +$$

$$+\left(\sqrt{t}\right)^1 \left[A_1 i^1 erfc\frac{\beta}{2a} + B_1 i^1 erfc\frac{-\beta}{2a}\right] +$$

$$+\left(\sqrt{t}\right)^2 \left[A_2 i^2 erfc\frac{\beta}{2a} + B_2 i^2 erfc\frac{-\beta}{2a}\right] + \cdots +$$

$$+\left(\sqrt{t}\right)^n \left[A_n i^n erfc\frac{\beta}{2a} + B_n i^n erfc\frac{-\beta}{2a}\right] =$$

$$= \sum_{n=0}^{\gamma} \mu_n t^{\frac{n}{2}}$$

where $\gamma = sup\{m,n\}$

for $x = \alpha\sqrt{t}$

$$u(\alpha\sqrt{t},t) \equiv (\sqrt{t})^0\left[A_0 i^0 erfc\frac{\alpha}{2a} + B_0 i^0 erfc\frac{-\alpha}{2a}\right] +$$
$$+(\sqrt{t})^1\left[A_1 i^1 erfc\frac{\alpha}{2a} + B_1 i^1 erfc\frac{-\alpha}{2a}\right] +$$
$$+(\sqrt{t})^2\left[A_2 i^2 erfc\frac{\alpha}{2a} + B_2 i^2 erfc\frac{-\alpha}{2a}\right] + \cdots +$$
$$+(\sqrt{t})^n\left[A_n i^n erfc\frac{\alpha}{2a} + B_n i^n erfc\frac{-\alpha}{2a}\right] =$$
$$= \sum_{n=0}^{\gamma} \nu_n t^{\frac{n}{2}}$$

Finally coefficients $A_0, A_1, A_2, \ldots, A_\gamma$ and $B_0, B_1, B_2, \ldots, B_\gamma$ are determined from system of linear equations

$$A_0 i^0 erfc\frac{\beta}{2a} + B_0 i^0 erfc\frac{-\beta}{2a} = \mu_0$$
$$A_0 i^0 erfc\frac{\alpha}{2a} + B_0 i^0 erfc\frac{-\alpha}{2a} = \nu_0$$
$$A_1 i^1 erfc\frac{\beta}{2a} + B_1 i^1 erfc\frac{-\beta}{2a} = \mu_1$$
$$A_1 i^1 erfc\frac{\alpha}{2a} + B_1 i^1 erfc\frac{-\alpha}{2a} = \nu_1$$
$$A_2 i^2 erfc\frac{\beta}{2a} + B_2 i^2 erfc\frac{-\beta}{2a} = \mu_2$$
$$A_2 i^2 erfc\frac{\alpha}{2a} + B_2 i^2 erfc\frac{-\alpha}{2a} = \nu_2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$A_\gamma i^\gamma erfc\frac{\beta}{2a} + B_\gamma i^\gamma erfc\frac{-\beta}{2a} = \mu_\gamma$$
$$A_\gamma i^\gamma erfc\frac{\alpha}{2a} + B_\gamma i^\gamma erfc\frac{-\alpha}{2a} = \nu_\gamma$$

where $i^\gamma erfc\frac{\beta}{2a}, i^\gamma erfc\frac{-\beta}{2a}, i^\gamma erfc\frac{\alpha}{2a}, i^\gamma erfc\frac{-\alpha}{2a}$, γ=0,1,2... are identified from tables.

Remark: One of key points in solving Heat Equations in the domains with moving boundaries of the first type is to correctly identify value of γ, which takes maximum value between m and k in the boundary conditions.

Example 1

Solve the given boundary-value problem using Integral Error Functions

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2}, \qquad -\infty < x < 4\sqrt{t}, \qquad t > 0 \tag{11}$$

$$u(x,0) = e^x, \tag{12}$$

$$u\left(4\sqrt{t},t\right) = 2\sqrt{t} + 4t, \tag{13}$$

$$u(-\infty,t) = 0 \tag{14}$$

Solution

Solution considered in the form

$$u(x,t) = \sum_{n=0}^{k} (\sqrt{t})^n \left[A_n i^n \operatorname{erfc} \frac{x}{2\sqrt{t}} + B_n i^n \operatorname{erfc} \frac{-x}{2\sqrt{t}}\right] \tag{15}$$

for t=0

$$\lim_{t\to 0} (2\sqrt{t})^n i^n erfc \frac{-x}{2\sqrt{t}} = \frac{2}{n!} x^n, \tag{16}$$

while

$$\lim_{t\to 0} (2\sqrt{t})^n i^n erfc \frac{x}{2\sqrt{t}} = 0 \tag{17}$$

Then initial condition (12) gives

$$\sum_{n=0}^{\infty} \frac{2}{n!} B_n x^n = \sum_{n=0}^{\infty} \frac{1}{n!} x^n ,$$

thus

$$B_n = \frac{1}{2} \tag{18}$$

And for $x = 4\sqrt{t}$

$$\sum_{n=0}^{k} (\sqrt{t})^n \left[A_n i^n erfc\, 2 + B_n i^n erfc\,(-2)\right] = 2\sqrt{t} + 4t \tag{19}$$

It is very important to choose right value of k. Particularly in this case, k will be equal to 2. Expression (19) will take the form

$$A_0 i^0 erfc\, 2 + \frac{1}{2} i^0 erfc\,(-2) +$$

$$+ t^{\frac{1}{2}} \left[A_1 i^1 erfc\, 2 + \frac{1}{2} i^1 erfc\,(-2)\right] +$$

$$+ t\left[A_2 i^2 erfc\, 2 + \frac{1}{2} i^2 erfc\,(-2)\right] = 2\sqrt{t} + 4t$$

where

$$A_0 = \frac{-\frac{1}{2} i^0 erfc\,(-2)}{i^0 erfc\, 2}, \quad A_1 = \frac{1 - \frac{1}{2} i^1 erfc\,(-2)}{i^1 erfc\, 2}, \quad A_2 = \frac{1 - \frac{1}{2} i^2 erfc\,(-2)}{i^2 erfc\, 2}$$

and $i^0 erfc\,(-2), i^1 erfc\,(-2), i^2 erfc\,(-2), i^0 erfc\, 2, i^1 erfc 2, i^2 erfc\, 2$ can be found in *erfc* tables.

LIST OF REFERENCES

1 Sarsengeldin, M. Analytical solution of the third boundary-value problem for the heat equation by IEF method. - «Поиск-Ізденіс», Kazakhstan, Almaty, сер. физ.- мат. наук, № 4(1), 2012.

2 Sarsengeldin, M. Mathematical Model of Arc Erosion in Silver-based Electrical Contacts. - Ulyanovsk, Russia, Электрические Аппараты и Электротехнические Комплексы и Системы. - Vols 2, (2012), pp. 16-23.

3 Харин, С. Н. // О тепловых задачах с подвижной границей. Известия АН Каз ССР, сер. физ.- мат. наук, № 3, 1965.

Suleiman Demirel University, Almaty.
Material received on 20.03.13.

М. М. Сарсенгельдин, Г. Коспанова

Бірінші шеткі есебінің ИҚФ (интегралды қателер функциясы) әдісі арқылы аналитикалық шешімі

Сулейман Демирел атындағы университеті, Алматы қ.
Материал 20.03.13 редакцияға түсті.

М. М. Сарсенгельдин, Г. Коспанова

Аналитическое решение уравнения теплопроводности ИФО (интегральная функция ошибок) методом

Университет имени Сулеймана Демиреля, г. Алматы.
Материал поступил в редакцию 20.03.13.

Бастапқы уақытта құлдырайтын, жылжымалы шекаралар аймақтарында, Дирихле шеткі есебінің аналитикалық шешімі.

Найдено аналитическое решение первой краевой задачи уравнения теплопроводности в областях с подвижными границами, вырождающимимся в начальный момент времени методом интегральной функции ошибок.

УДК 532.456

А. А. Топчубаев, У. М. Туганбаев

АНАЛИТИЧЕСКОЕ ИССЛЕДОВАНИЕ УРАВНЕНИЯ КОНВЕКТИВНОЙ ДИФФУЗИИ

В работе исследуется нестационарное уравнение конвективной диффузии. На основании метода малых возмущений, это уравнение записано как линейное и его решение найдено в автомодельном виде и определены два класса решений.

Основываясь на принципах геохимической гидродинамики и результатах её применения в области орошения, осушения земель в работе исследуется и изложена методика расчета солевого режима почвогрунтов. В соответствии с этим, аналитически исследуется уравнение конвективной диффузии и массообмена при фильтрации воды в почвогрунтах, предлагаются методы расчета этих процессов.

В районах орошения важной проблемой является предупреждение засоления плодородных земель, вышедших из сельхозоборота вследствии подъема минерализованных грунтовых вод и другого рода засоления. Остается актуальным также рассоление земель, засоленных в естественных условиях, которые после опреснения становятся пригодными для земледелия. Рассоление таких земель осуществляется посредством промывок пресной водой или слабо минерализованной водой до порогов токсичности и понижения уровня соленых вод с помощью дренажа. Опыт освоения и орошения земель показывает, что к засоленным почвам необходимо относить почвы не только в районе корней растений, но и земли с легко растворимыми солями в количестве, которые могут сконцентрироваться в верхних слоях почвы до пределов, превышающих порог токсичности. Поэтому важнейшее значение приобретают мероприятия, предупреждающие засоление почв, прогнозировать и правильно вести расчеты последствий орошения земель. Применение мелиоративных мероприятий существенно воздействует на естественный гидрохимический режим верхней части почвы, которые могут вызвать серьезные последствия экологического

характера. Поэтому исключительно важна разработка хороших методов прогноза гидрохимических процессов в почвах, грунтах зоны аэрации и в грунтовых водах. Прогноз должен объяснить, почему одно и тоже мероприятие, в одних условиях дает высокий эффект, а в других оказывается слабо эффективным, а иногда и вредным. Правильный прогноз основывается на методах геохимической гидродинамики, которая объединяет в себе принципы теории фильтрации, диффузии, химической кинетики и современной математики. Итак, движение солей в почвогрунтах происходит вследствии миграции их с растворителями. Этот процесс солепереноса в почвогрунтах, при отсутствии химической реакции и сорбции описывается следующим уравнением [1]

$$m_0 \frac{\partial C}{\partial t} = \frac{\partial}{\partial x}\left(D(C)\frac{\partial C}{\partial x}\right) + \frac{\partial}{\partial y}\left(D(C)\cdot\frac{\partial C}{\partial y}\right) + \frac{\partial}{\partial z}\left(D(C)\frac{\partial C}{\partial z}\right) - \mathrm{div}(vC), \quad (1)$$

здесь функция $C(x,y,z,t)$- концентрация соли в жидкости, v-скорость фильтрации, m_0 – активная пористость грунта, характеризует активный объем порового пространства, $D(C)$- коэффициент диффузии, которая в общем случае является функцией от концентрации соли в жидкости.

Ранее предлагали, что почва считается однородной, изотропной, поэтому в первом приближении коэффициент диффузии и компоненты скорости фильтрации считали постоянными. В этом случае, уравнение (1) имело вид

$$m_0 \frac{\partial C}{\partial t} = D_0\left[\frac{\partial^2 C}{\partial x^2} + \frac{\partial^2 C}{\partial y^2} + \frac{\partial^2 C}{\partial z^2}\right] - U_0\frac{\partial C}{\partial x} - V_0\frac{\partial C}{\partial y} - W_0\frac{\partial C}{\partial z}, \quad (2)$$

а ставились следующие начально – краевые условия:

а. В начальный момент $t = t_0$, $C(x, y, x, t_0) = P_0(x, y, z)$ (3)

б. На границе Г $C(x, y, z, t_0) = Q_0(x_0, y_0, z_0, t)$. (4)

Далее, ввели новую функцию [2]

$$C(x, y, x, t_0) = \exp\xi_0 \cdot Q(x, y, z, t), \quad \xi_0 = a_0 x + b_0 y + c_0 z + d_0 t, \quad (5)$$

и получили линейное уравнение вида

$$Q_\tau = Q_{xx} + Q_{yy} + Q_{zz}, \quad (6)$$

которое является уравнением дальнейших исследований, при этом

$$a_0 = \frac{U_0}{2D_0}, \quad b_0 = \frac{V_0}{2D_0}, \quad C_0 = \frac{W_0}{2D_0}, \quad d_0 = -\frac{U_0^2 + V_0^2 + W_0^2}{4m_0 D_0}, \quad \tau = \frac{D_0}{m_0} t.$$

Решение уравнения (6), инвариантно относительно однопараметрической группы преобразования подобия

$$x \Rightarrow \gamma x, \qquad y' \Rightarrow \gamma y, \qquad z' \Rightarrow \gamma z, \qquad \tau' \Rightarrow \gamma \tau, \qquad Q^1 \Rightarrow \gamma Q,$$

которое должно иметь вид

$$Q(x, y, z, \tau_0) = \tau^n \cdot P(\eta_1), \quad \eta_1 = (x^2 + y^2 + z^2)/\tau. \tag{7}$$

Находя все необходимые частные производные и подставляя в рассматриваемое уравнение (6), получим следующее обыкновенное дифференциальное уравнение

$$P''(\eta_1) + \left[\frac{1}{2} + \frac{1}{4}\eta_1\right] P'(\eta_1) - \frac{n}{4} P(\eta_1) = 0. \tag{8}$$

Если сравнить его с уравнением вида [2]

$$xy'' + (ax + b)y' + (cx + d)y = 0. \tag{9}$$

то можно записать одно из решений в форме

$$y = x^{-b/2} \cdot e^{-ax/2} \cdot F\left(\frac{2d - ab}{2\sqrt{a^2 - 4c}}\right), \qquad \frac{1}{2}(b-1); \qquad x\sqrt{a^2 - 4c}, \tag{10}$$

т. е. одно из частных решений уравнения (8) принимает форму

$$P(\eta_1) = \eta_1^{-1,4} \cdot e^{-\eta_1/8} \cdot F\left(-\frac{4n+1}{4}, -\frac{1}{4}; \frac{1}{4}\eta_1\right) \tag{11}$$

где $a = \frac{1}{4}, \quad b = \frac{1}{2}, \quad c = 0, \quad d = -\frac{к}{4}.$

Последнее решение можно записать в виде полинома при, $к = (4n-1)/4$. Решение, изучаемого уравнения (6), в общем виде, запишется $\eta_1 = (x^2 + y^2 + z^2)/\frac{D_0}{m_0} t,$

$$C(x, y, z, t) = \exp\eta_1 \cdot \left(\frac{D_0}{m_0} t\right)^n \cdot \left[\eta_1^{-1/4}\right] \cdot \exp\eta_1 \cdot F\left(-\frac{4n+1}{4}, \frac{1}{4}, \frac{1}{4}\eta_1\right) \tag{12}$$

Если ввести новую переменную $\eta = -\eta_1/4$, тогда определяя первую и вторую производную P_1', P_1'' и подставляя в (8), получим выражение

$$\eta P''(\eta) + \left[\frac{1}{2} - \eta\right] \cdot P_1'(\eta) + nP_1(\eta) = 0, \qquad (13)$$

которое является вырожденным гипергеометрических уравнением Гаусса и имеет два линейно – независимых решения

$$P_1(\eta) = C_1 F_1\left(-n, \frac{1}{2}; \eta\right) + C_2 \eta^{1/2} F_2\left(-\eta + \frac{1}{2}, \frac{3}{2}; \eta\right) \qquad (14)$$

Известно, что оба линейно – независимые решения одновременно не могут быть записаны в виде алгебраического многочлена. Первое решение имеет вид полинома когда, $n = 1,2,3....K$, а второе при $n = 3/2,5/2,\ldots.(2\kappa+1)/2$.

Можем записать некоторые точные решения для первого решения уравнения (6) с учетом запланированного решения (7)

$$\begin{aligned}
&Q(x,y,z,\tau) = C_1(2\tau + \eta^2), && \text{при } n = 1,\\
&Q(x,y,z,\tau) = C_1(12\tau^2 + 12\tau\eta + \eta^4), && \text{при } n = 2,\\
&Q(x,y,z,\tau) = C_1(120\tau^3 + 180\tau^2\eta + 30\tau\eta^4 + \eta^6), && \text{при } n = 3,\\
&Q(x,y,z,\tau) = C_1(a_0\tau^k + a_1\tau^{k-1}\eta + \ldots a_{n-1}\tau^{2n-2} + a_n\eta^{2n}), && \text{при } n = k.
\end{aligned} \qquad (15)$$

Для второго линсйно – независимого решения уравнения (6), имеем другие выражения

$$\begin{aligned}
&Q(x,y,z,\tau) = C_2\eta(6\tau + \eta^2), && \text{при } n = 3/2,\\
&Q(x,y,z,\tau) = C_2\eta(60\tau^2 + 20\tau\eta^2 + \eta^4), && \text{при } n = 5/2,\\
&Q(x,y,z,\tau) = C_2\eta(80\tau^3 + 420\tau^2\eta^2 + 42\tau\eta^4 + \eta^6), && \text{ïðè } n = 7/2,\\
&Q(x,y,z,\tau) = C_2\eta(b_0\tau^{k-1/2} + b_1\tau^{k-3/2}\eta^2 + \ldots b_{n-1}\tau\eta^{2k-3/2} + b_n\eta^{2k+1/2}), && \text{при } n = n+1/2.
\end{aligned} \qquad (16)$$

Таким образом, нами разработаны два класса частных автомодельных решения для уравнения (6), которые имеют множество различных решений при различных n. Если использовать преобразования Куммера, то можно найти другие классы частных решений.

Рассмотрим другое решение уравнения (6), исходя из групповых свойств дифференциальных уравнений [2], при котором соблюдается

инвариантность рассматривасмого уравнения относительно группы преобразования независимых и зависимых переменных. Исходя из вышесказанного, решение уравнения (6), можно найти в форме

$$Q(x,y,z,\tau)=(x+y+z)^2\cdot f(\xi_1),\qquad \text{где}\quad \xi_1=\frac{\tau}{(x+y+z)^2} \tag{17}$$

Находя все необходимые частные производные, подставляя их в уравнение, получим обыкновенное дифференциальное уравнение второго порядка

$$\xi_1^2 f_0''(\xi_1)-\left[\frac{1}{12}+\left(n-\frac{3}{2}\right)\xi_1\right]f'(\xi_1)+\frac{n(n-1)}{4}f(\xi_1)=0. \tag{18}$$

С введением новой функции [4]

$$f'(\xi_1)=e^{\xi}\cdot\xi^{\nu}f_0(\xi),\quad \text{где}\quad \xi=\xi_1^{-1} \tag{19}$$

получим следующее уравнение

$$\xi^2 f_0''(\xi)+\left[\frac{25}{12}\xi^2+\left(2\nu+\frac{1}{2}+n\right)\xi\right]f_0'(\xi)+\left[\frac{13}{12}\xi^2+\left(n+\frac{1}{2}+\frac{25}{12}\nu\right)\xi\right]\cdot f_0(\xi)+$$

$$+\left[\frac{n(n-1)}{4}+\left(n-\frac{1}{2}\right)\nu+\nu^2\right]f_0(\xi)=0. \tag{20}$$

Предположим, что квадратная скобка последнего члена, полученного уравнения равно нулю. Это возможно при $\nu_1=-n/2$ и $\nu_2=(1-n)/2$ и поэтому для каждого значения ν имеем следующие два уравнения называемыми вырожденными гипергеометрическими уравнениями Гаусса

$$\xi f_0''+\left[\frac{1}{2}+\frac{25}{12}\xi\right]f_0'+\left[\frac{13}{12}\xi-\frac{n-12}{24}\right]f_0=0,\quad \text{при}\quad \nu_1=-\frac{n}{2} \tag{21}$$

$$\xi f_0''+\left[\frac{3}{2}+\frac{25}{12}\xi\right]f_0'+\left[\frac{13}{12}\xi-\frac{n-37}{24}\right]f_0=0,\quad \text{при}\quad \nu_1=-\frac{n-1}{2}. \tag{22}$$

В окрестности особой точки $\xi=0$, оба линейно – независимые решения уравнения (21) запишутся

$$f_0(\xi)=\exp\left(-\frac{13}{12}\xi\right)\cdot\left[C_1F\left(\frac{n+1}{2},\frac{1}{2};\frac{\xi}{12}\right)+C_2\xi^{1/2}F\left(\frac{n+2}{2},\frac{3}{2};\frac{\xi}{12}\right)\right], \tag{23}$$

где C_1, C_2 - постоянные интегрирования.

Общее решение уравнения (6), с учетом решения (17,19), примет вид

$$Q(x,y,z,\tau)=\tau^{n/2}\cdot\exp(-\xi/12)\cdot\left[C_1F\left(\frac{n+1}{2},\frac{1}{2};\frac{\xi}{12}\right)+C_2\xi^{1/2}\cdot F\left(\frac{n+2}{2},\frac{3}{2};\frac{\xi}{12}\right)\right] \qquad (24)$$

Таким образом, искомая функция для уравнения (21), окончательно запишется

$$C(x,y,z,\tau)=\exp(a_0x+b_0y+c_0z-d_0t)\cdot\left(\frac{D_0t}{m_0}\right)^{n/2}\cdot\exp\left(\frac{(x+y+z)^2}{D_0+12t}\cdot m_0\right)\cdot \qquad (25)$$

$$\cdot\left\{C_1F\left[\frac{n+1}{2},\frac{1}{2};\frac{m_0}{12D_0}\cdot\left(\frac{x+y+z}{t}\right)^2\right]+C_2\left(\frac{m_0}{12D_0}\frac{(x+y+z)^2}{t}\right)^{1/2}F\left[\frac{n+2}{2},\frac{3}{2};\frac{m_0}{12D_0}\frac{(x+y+z)^2}{t}\right]\right\}$$

Общее решение, для уравнения (22), примет форму

$$f_0(\xi)=\exp\left(-\frac{13}{12}\xi\right)\cdot\left[C_1F\left(\frac{n+2}{2},\frac{3}{2};\frac{\xi}{12}\right)+C_2\xi^{-1/2}F\left(\frac{n+1}{2},\frac{1}{2};\frac{\xi}{12}\right)\right], \qquad (26)$$

тогда для самого уравнения (6), запишем его решение

$$Q(x,y,z,\tau)=\left(\frac{m_0}{D_0}\tau\right)^{\frac{n}{2}}(x,y,z,\tau)\exp\left(-\frac{\xi}{12}\right)\cdot\left[C_1F\left(\frac{n+2}{2},\frac{3}{2};\frac{\xi}{12}\right)+C_2\xi^{-1/2}F\left(\frac{n+1}{2},\frac{1}{2};\frac{\xi}{12}\right)\right] \qquad (27)$$

а с учетом выражения (5), окончательно имеем

$$C(x,y,z,t)=\exp(a_0x+b_0y+c_0z-d_0t)\cdot t^{\frac{n-1}{2}}(x+y+z)\cdot\exp\left(-\frac{m_0}{12D_0}\frac{(x+y+z)^2}{t}\right)\cdot$$

$$\cdot\left[C_1F\left(\frac{n+2}{2},\frac{3}{2};\frac{m_0}{12D_0}\frac{(x+y+z)^2}{t}\right)+C_2\left(\frac{m_0}{12D_0}\frac{(x+y+z)^2}{t}\right)^{-1/2}\cdot\right.$$

$$\left.\cdot F\left(\frac{n+1}{2},\frac{1}{2};\frac{m_0}{12D_0}\frac{(x+y+z)^2}{t}\right)\right] \qquad (28)$$

Теперь рассмотрим случаи, когда каждое частное решение вырожденной гипергеометрической функции Гаусса может быть представимо в виде алгебраического выражения. Первое частное решение выражения (23) представляется в форме полинома, когда $n=-2k+1$, а второе при $n=-2k-2$.

Отсюда видно, что при одних и тех же значениях показателя автомодельности, частные решения не могут быть одновременно записаны в алгебраических полиномах. Определим некоторые точные решения уравнения (6). Рассмотрим для первого частного решения для искомой функции $C(x,y,z,t)$ его выражения, при $n=-1$ и $n=-3$

$$C(x,y,z,t)=\exp(a_0x+b_0y+c_0z-d_0t)\cdot\left(\frac{D_0}{m_0}t\right)^{-1/2}\cdot\exp\left(-\frac{m_0(x+y+z)^2}{12D_0t}\right) \tag{29}$$

$$C(x,y,z,t)=\exp(a_0x+b_0y+c_0z-d_0t)\cdot\left(\frac{D_0}{m_0}t\right)^{-3/2}\cdot$$

$$\cdot\exp\left(-\frac{m_0(x+y+z)^2}{12D_0t}\right)\cdot\left[1-\frac{m_0(x''+y+z)^2}{6D_0\cdot t}\right]. \tag{30}$$

Теперь выпишем два решения при $n=-2$ и $n=-4$, для второго частного решения

$$C(x,y,z,t)=C_2\left(\frac{D_0}{m_0}t\right)^{3/2}\cdot(x+y+z)\cdot\exp\left[(a_0x+b_0y+c_0z+d_0t)\frac{m_0(x+y+z)^2}{12D_0t}\right] \tag{31}$$

$$C(x,y,z,t)=C_2\left(\frac{D_0}{m_0}t\right)^{5/2}\cdot(x+y+z)\cdot\exp\left[a_0x+b_0y+c_0z-d_0t-\frac{m_0(x+y+z)^2}{12D_0t}\right]\cdot$$

$$\cdot\left[1-\frac{m_0(x+y+z)^2}{18D_0t}\right] \tag{32}$$

Таким образом, нами определен класс точных решений уравнения (2.6), причем анализ полученных решений убеждает нас, что с уменьшением показателя автомодельности n число слагаемых, получаемых полиномов, увеличивается. Постоянные интегрирования C_1, C_2 определяется из явного задания начально – краевых условий (3,4).

СПИСОК ЛИТЕРАТУРЫ

1. **Полубаринова-Кочина, П. Я., и др.** О движении почвенной влаги грунтовых вод и солей. «Кулундин. стень и вопросы её мелиор-и». – Новосибирск. 1962.

2. **Туганбаев, У. М., Топчубаев, А. А., Турусбекова, Н. О.** К моделированию переноса солей в почвогрунтах фильтрационным потоком и её исследование. // Вестник, КГУ им. И. Арабаева., серия: физика, математика и информатика. – 2012. – С. 113-118.

3. **Овсянников, Л. В.** Грунтовой анализ дифференциальных уравнений в частных производных. – М. : Наука, 1978 – 400 с.

4. **Камке, Э.** Справочник по обыкновенным дифференциальным уравнениям. – М. : Наука, 1976. – 576 с.

Кыргызский национальный аграрный университет
имени К. И. Скрябина, г. Бишкек, Кыргызская Республика.
Материал поступил в редакцию 04.09.13.

А. А. Топчубаев, У. М. Туганбаев

Конвективті араласу теңдеуінің аналитикалық зерттеуі

К. И. Скрябин атындағы Қырғыз ұлттық аграрлық университеті,
Бишкек қ., Қырғыз Республикасы.
Материал 04.09.13 редакцияға түсті.

A. A. Topchubaev, U. M. Tuganbaev

Analytical research of the eguation of convectiv diffusion

National Agrarian University named after K. I. Skryabin,
Bishkek, Kyrgyzstan.
Material received on 04.09.13.

Жұмыста конвективті араласудың стационарлы емес теңдеуі зерттеледі. Кіші қозулардың әдісі негізінде бұл теңдеу желілік ретінде жазылған, оның шешімі автомодельді түрде табылған және екі жіктеудегі шешімі анықталған.

In work the non-stationary equation of convective diffusion is investigated. On the basis of a method of small indignations, this equation is written down as linear and its decisions is found in an auto modeling king and two classes of decisions are defined.

УДК 373.51

З. В. Хотянович

ДИФФЕРЕНЦИРОВАННЫЕ УПРАЖНЕНИЯ ПО ГЕОМЕТРИИ В 8 КЛАССЕ

Разработаны упражнения прикладного и творческого характера по геометрии для учащихся средней школы. Задание направлены на практическую подготовку учащихся, учать исследовательской деятельности.

Раздел предназначен для организации дифференцированной работы учащихся при обучении геометрии в 8 классе. Задания соответствуют порядку изложения материала в учебнике геометрии Ж. Кайдасова (Геометрия: Учебник для 8 кл. общеобразовательных школ-2 изд./ Ж. Кайдасов, Г. Хабарова, А. Абдиев. – Алматы: Мектеп, 2012 г. – 112 стр., ил.) Упражнения помогут разнообразить задачи учебника.

Раздел содержит упражнения прикладного характера, иллюстрирующие применение геометрии в различных областях человеческой деятельности. Упражнения сгруппированы по темам учебника, уровням овладения материалом в прикладной направленности содержания.

Задания могут быть использованы для диагностики познавательных интересов учащихся.

Классифицируя упражнения по уровням овладения материалом, каждое из них можно отнести к обязательному, повышенному или творческому уровням.

Площади многоугольников

Площадь прямоугольника

1[1].Выполните вычисления.

а) Мальчик на лыжах стоит на снегу. Вычислите давление, которое он оказывает на снег. Масса мальчика равна 40 кг, длина лыжи-1,5 м, ширина лыжи-7см.

Решение: S=150 см * 7 см =1050 см^2=0,105 м^2

N= mqS= 40 кг* 10 м/с^2 * 0,105 м^2 = 42,000 Н= 42 Н

б) Вам нужно покрасить прямоугольный пол в комнате шириной 3 м и длиной 5,5 м. Вычислите стоимость необходимой массы краски. На окраску 1 $м^2$ пола расходуется примерно 200 г краски. Цена 1 кг краски равна 15 рублям.

в) У вас есть 2 пакстика семян редиса весам по 10 г. Подсчитайте, какое количество прямоугольных грядок длиной 3 м шириной 60 см можно засадить этими семенами. Известно, что расход семян составляет 3,5 г на 1$м^2$.

г) Древний индийский храм Кайласа Натхи высечен из скалы в 8 в.н.э. Размеры прямоугольной площадки, на которой стоит храм, равны 87 м х 47м, а прямоугольника в основании здания-61 м х 33 м. Какую часть площадки занимает храм?

1^2.а) Вычислите давление на землю стоящего горизонтально легкового автомобиля.

б) Вычислите стоимость краски, требуемой для окраски стен вашей комнаты.

в) Комната нормально освещена, если отношение площади окна к площади пола не менее 0,2. Нормально ли освещена ваша комната?

г) Какую площадь занимает дом, в котором вы живете?

Площадь треугольника

2^1. а) Вычислите площадь крыши дома (см.вид сверху на рис. 1).

(Рис.1)

Она состоит из четырех равных равнобедренных треугольников с основанием в 6,7 м и высотой в 4,4 м. Рис.1

б) Вычислите площадь Бермудского треугольника (рис.2). Будем считать его равносторонним со стороной равной 1700 км и высотой 1472 км.

Рис. 2

в) Вычислите площадь поверхности кристалла искусственного алмаза. Кристалл представляет собой октаэдр. (рис.3): его поверхность состоит из восьми равных равносторонних треугольников со стороной 1 мм и высотой 0,9 мм.

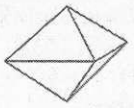


Рис. 3

Рис.4

г) Вычислите площадь паруса лодки. Парус имеет форму треугольника (рис.4) с основанием 2 м и высотой 5 м.

2^2. Решите задачу.

а) Вычислите массу плоской железной детали (рис. 5). Толщина детали равна 0,5 см, плотность железа-7,8 г/см?. Размеры детали указаны в сантиметрах.

б) Вычислите стоимость ткани по цене 10 рублей за $1м^2$, необходимой для раскроя фартука с одинаковым квадратными карманами по данной выкройке (рис. 6). Размеры ткани на рисунке указаны в сантиметрах.

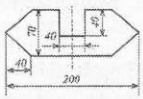


Рис.5

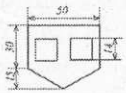


Рис. 6

в) Вычислите объем воды, требующейся для полива огорода (рис.7). Известно, что на 1 $м^2$ площади огорода расходуется 5 л воды. Размеры указаны в метрах.

г) Вычислите массу краски, которая потребуется для изображения орнамента на стене здания (рис.8). известно, что на 1 $м^2$ расходуется 200 г краски. Размеры орнамента указаны в сантиметрах.

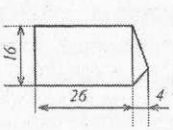


Рис.7

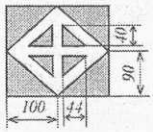


Рис.8

Площадь трапеции

3^1. а) Вычислите площадь крыши (вид прямо и вид сверху см. на (рис.9).

б) Вычислите площадь «живого сечения» канала (рис. 10). «Живым сечением» канала (реки) называют поперечное сечение его русла.

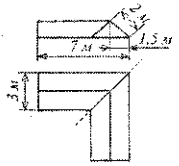


Рис.9

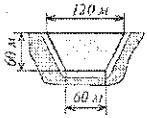


Рис.10

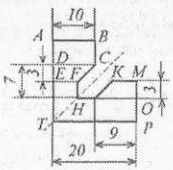
3^2. а) Четырехскатная крыша состоит из двух одинаковых трапеций и двух одинаковых треугольников. Длина прямоугольника в основании крыши равна 25 м, ширина-12 м, длина гребня-19 м, высота трапеции - 7,5 м, высота треугольника, опущенная на основание, равна 5,4 м. Выполните рисунок развертки крыши в удобном масштабе, если оснавания трапеции больше основания треугольника. Вычислите площадь крыши.

б) Штат Невада США имеет вид прямоугольный трапеции, от которой отсечена маленькая прямоугольная трапеция. Острые углы трапеций совпадают. Северная граница штата длиной 480 км является высотой первой трапеции, западная – длиной 350км – меньшим основанием, восточная длиной 820 км – большим основанием. Юго-восточная граница идет по реке Колорадо, отсекающей трапецию высотой 60 км, основаниями 100 км и 160 км. Сделайте рисунок в удобном масштабе. Вычислите площадь штата.

в) Крыло летучей мыши состоит из трех многоугольников. Два из них – треугольники с общей стороной и высотой, равной 3 см, а основаниями – по 2,2 см. Один из треугольников равнобедренный с боковой стороной в 3,2 см, которая совпадает с оснаванием прямоугольной трапеции. Другое основание трапеции имеет длину 2,4 см, а ее высота равна 1,5 см. Выполните рисунок крыла в удобном масштабе. Вычислите площадь крыльев мыши.

г) В рассказе Л.Н. Толстого «Много ли человеку земли нужно» крестьянин Пахом старался обежать за день как можно больше земли, чтобы получить ее во владение. Пахом обежал прямоугольную трапецию с основаниями, равными 2 и 10 верст, и высотой 13 верст. Сделайте рисунок в удобном масштабе. Вычислите площадь земли Пахома.

Площадь многоугольника



4^1. а) Вычислите площадь детали по данным рисунка 11. Деталь симметрична относительно прямой *TH*. Размеры указаны в сантиметрах.

Рис.11

б)Вычислите площадь нижней поверхности морской звезды, используя данные рисунка 12. Размеры указаны в сантиметрах.

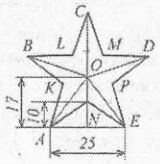


Рис. 12

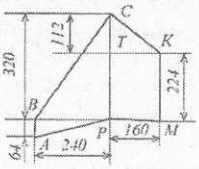


Рис. 13

в) Вычислите площадь Московского Кремля во времена Юрия Долгорукого, используя план на рисунке 13. Размеры указаны в метрах.

4^2. Перенесите один из рисунков упражнения 4^1 в тетрадь в удобном масштабе. Предложите три варианта вычесления требуемой площади. Вычеслите площадь многоугольника наиболее рациональным способом.

4^3. Изобразите в тетради одну из предложенных ниже фигур в удобном масштабе. Вычислите приближенно ее площадь, заменив данную фигуру наиболее подходящим многоугольником:

а) лобовое стекло легкового автомобиля;

б) любое государство мира (изображение на карте);

в) лист дерева;

г) Древняя Русь (изображение на карте).

СПИСОК ЛИТЕРАТУРЫ

1 **Александров, А. Д. и др.** Геометрия для 8-9 классов: Учеб. Пособие для учащихся шк. и классов с углубл. изуч. математики / А. Д. Александров, А. Л. Вернер, В. И. Рыжик. – М. : Просвещение, 1991. – 451 с.: ил.

2 **Бекбоев, И. Б.** Задачи с практическим содержанием как средство раскрытия содержательно-прикладного значения математики в восьмилетней школе. – Фрунзе, 1967. – 156 с.

3 **Перельман, Я. И.** Занимательная геометрия. – М. : Триада-Литера, 1994. – 327 с.

Средняя общеобразовательная школа № 43, г. Павлодар.
Материал поступил в редакцию 29.04.13.

З. В. Хотянович

8-ші сыныпта геометрия бойынша сараланған жаттығулар

№ 43 ЖОББМ, Павлодар қ.
Материал 29.04.13 редакцияға түсті.

Z. V. Khotyanovich

Differentiated exercises on geometry in 8th grade

Secondary comprehensive school № 43, Pavlodar.
Material received on 29.04.13.

НАШИ АВТОРЫ

Алдабергенов Фазылхан Селиханович – учитель черчения высшей категории, СОШ №12, методист городского отдела образования, г. Экибастуз.

Баланюк Алена Ивановна – учитель математики и физики 2-й категории, СОШ № 43, г. Павлодар.

Будкова Валентина Олеговна – магистрант, кафедра математики, Павлодаский государственный университет имени С. Торайгырова, г. Павлодар.

Дроботун Борис Николаевич – Член корреспондент АПН РК, к.ф.-м.н., д.п.н., профессор ККСОН, профессор кафедры математики, Павлодаский государственный университет имени С. Торайгырова, г. Павлодар.

Дыйканова Айнура Тынчыбековна – старший преподаватель, Кыргызский национальный аграрный университет имени К. И. Скрябина, г. Бишкек, Кыргызская Республика.

Амренова Гулсара Жумабаевна – учитель математики, школа имени Абая, Лебяжинский район, г. Павлодар.

Жумалиев Т. Ж. – Кыргызский национальный аграрный университет имени К. И. Скрябина, г. Бишкек, Кыргызская Республика.

Жумаш Айжан Нурлановна – студент, Павлодаский государственный университет имени С. Торайгырова, г. Павлодар.

Зейнулина Айман Файзулловна – к.ф.н., профессор, заведующая кафедрой практического курса казахского языка, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар.

Испулов Нурлыбек Айдаргалиевич – к.ф.-м.н., доцент, декан факультета физики, математики и информационных технологий, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар.

Коспанова Г. – Университет имени Сулеймана Демиреля, г. Алматы

Мурат Гулнар – магистрант, кафедра Математики, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар.

Мухамедзянова Нина Ивановна – магистр математики, старший преподаватель, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар.

Мухтаров Магзум – професор, кафедра Математики, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар.

Оралов Евгений Шакарович – магистрант, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар.

Павлюк Иван Иванович – к.ф.-м.н., профессор, кафедра Математики, Павлодарский университет имени С. Торайгырова, г. Павлодар.

Панасенко Ольга Игоревна – магистрант, Павлодарский университет имени С. Торайгырова, г. Павлодар.

Сагындыкова Р. К. – Кыргызский национальный аграрный университет имени К. И. Скрябина, г. Бишкек, Кыргызская Республика.

Садыкова Ризагуль Сембаевна – магистрант, кафедра Математики, Павлодарский университет имени С. Торайгырова, г. Павлодар.

Сарсембаева Галия Абаевна – студент, Павлодарский университет имени С. Торайгырова, г. Павлодар.

Сарсенгельдин М.М. – Университет имени Сулеймана Демиреля, г. Алматы.

Сейтханова Айнур Кусбековна – *к.ф.-м.н., старший преподаватель, кафедра физики и приборостроения,* Павлодарский государственный университет имени С. Торайгырова, г. Павлодар.

Топчубаев А. А. – Кыргызский национальный аграрный университет имени К. И. Скрябина г. Бишкек, Кыргызская Республика.

Туганбаев Уланбек Мансурович – д.ф.-м.н., профессор, Кыргызский национальный аграрный университет имени К. И. Скрябина, г. Бишкек. Кыргызская Республика.

Хамитов Мейрам Хамитович – академик, професор, кафедра Математики, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар.

Хотянович З. В. – учитель математики I категории, СОШ № 43, г. Павлодар.

ПРАВИЛА ДЛЯ АВТОРОВ НАУЧНЫЙ ЖУРНАЛ ПГУ ИМЕНИ С. ТОРАЙГЫРОВА («ВЕСТНИК ПГУ», «НАУКА И ТЕХНИКА КАЗАХСТАНА», «КРАЕВЕДЕНИЕ»)

1. В журналы принимаются статьи по всем научным направлениям в 1 экземпляре, набранные на компьютере, напечатанные на одной стороне листа с межстрочным интервалом 1,5, с полями 30 мм со всех сторон листа, электронный носитель со всеми материалами в текстовом редакторе «Microsoft Office Word (97, 2000, 2007, 2010) для WINDOWS».

2. Общий объем статьи, включая аннотацию, литературу, таблицы, рисунки и математические формулы не должен превышать **8-10 страниц.**

3. Статья должна сопровождаться рецензией доктора или кандидата наук для авторов, не имеющих ученой степени. Для статей, публикуемых в журнале «Вестник ПГУ» химико-биологической серии, требуется экспертное заключение.

4. Периодичность издания журналов – два раза в год (№1 – с января по июнь; №2 – с июля по декабрь)

Статьи должны быть оформлены в строгом соответствии со следующими правилами:

1. УДК по таблицам универсальной десятичной классификации;

2. Инициалы и фамилия (-и) автора (-ов), абзац по левому краю;

3. Название статьи – на казахском, русском и английском языках, заглавными буквами жирным шрифтом, абзац по левому краю;

4. Резюме на казахском, русском и английском языках: кегль – 10 пунктов, курсив, отступ слева-справа – 3 см, интервал 1,0 (см. образец);

5. Текст статьи: кегль – 14 пунктов, гарнитура – Times New Roman (для русского, английского и немецкого языков), KZ Times New Roman (для казахского языка).

6. Межстрочный интервал 1,5 (полуторный);

7. Список использованной литературы (ссылки и примечания в статье обозначаются сквозной нумерацией и заключаются в квадратные скобки). Статья и список литературы должны быть оформлены в соответствии с ГОСТ 7.5-98; ГОСТ 7.1-2003 (см. образец).

На отдельной странице

В бумажном и электронном вариантах приводятся:

– **название статьи, сведения об авторе: - Ф.И.О. полностью, ученая степень, ученое звание и место работы на казахском, русском и английском языках (для публикации в разделе «Наши авторы» и «Содержание»);**

– **полные почтовые адреса, номера служебного и домашнего телефонов, E-mail (для связи редакции с авторами, не публикуются);**

1. Иллюстрации, перечень рисунков и подрисуночные надписи к ним представляют по тексту статьи. В электронной версии рисунки и иллюстрации представляются в формате TIF или JPG с разрешением не менее 300 dpi.

2. Математические формулы должны быть набраны в Microsoft Equation Editor (каждая формула – один объект).

3. Автор просматривает и визирует грани статьи и несет ответственность за содержание статьи.

4. Редакция не занимается литературной и стилистической обработкой статьи. Рукописи не возвращаются. Статьи, оформленные с нарушением требований, к публикации не принимаются и возвращаются авторам.

5. Оплата за публикацию в научном журнале составляет 5000 (Пять тысяч) тенге.

Статью (бумажная, электронная версии, оригинал квитанции об оплате) следует направлять по адресу: 140008, Казахстан, г. Павлодар, ул. Ломова, 64, Павлодарский государственный университет имени С. Торайгырова, Издательство «Кереку», каб. 137.

Тел. 8 (7182) 67-36-69, (внутр. 1147), факс: 8 (7182) 67-37-05.

E-mail: kereky@mail.ru

Наши реквизиты:

РГП на ПХВ Павлодарский государственный университет имени С. Торайгырова РНН 451800030073 БИН 990140004654	РГП на ПХВ Павлодарский государственный университет имени С. Торайгырова РНН 451800030073 БИН 990140004654
АО «Цеснабанк» ИИК KZ57998FTB00 00003310 БИК TSESKZK A Кбе 16 Код 16	АО «Народный Банк Казахстана» ИИК KZ156010241000003308 БИК HSBKKZKX Кбе 16 Код 16

ОБРАЗЕЦ К ОФОРМЛЕНИЮ СТАТЕЙ:

УДК 316:314.3

А. Б. ЕСИМОВА

СЕМЕЙНО-РОДСТВЕННЫЕ СВЯЗИ КАК СОЦИАЛЬНЫЙ КАПИТАЛ В РЕАЛИЗАЦИИ РЕПРОДУКТИВНОГО МАТЕРИАЛА

В настоящей статье автор дает анализ отличительных особенностей репродуктивного поведения женщин сквозь призму семейно-родственных связей.

На современном этапе есть тенденции к стабильному увеличению студентов с нарушениями в состоянии здоровья. В связи с этим появляется необходимость корректировки содержания учебно-тренировочных занятий по физической культуре со студентами, посещающими специальные медицинские группы в.....

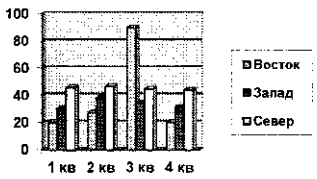
Продолжение текста публикуемого материала.

Пример оформления таблиц, рисунков, схем:

Таблица 1 – Суммарный коэффициент рождаемости отдельных национальностей

	СКР, 1999 г.	СКР, 1999 г.
Всего	1,80	2,22

Диаграмма 1 – Показатели репродуктивного поведения



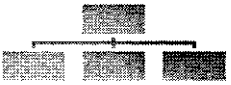


Рисунок 1 – Социальные взаимоотношения

СПИСОК ЛИТЕРАТУРЫ

1 **Эльконин, Д. Б.** Психология игры [Текст] : научное издание / Д. Б. Эльконин. – 2-е изд. – М. : Владос, 1999. – 360 с. – Библиогр. : С. 345–354. – Имен. указ. : С. 355–357. – ISBN 5-691-00256-2 (в пер.).

2 **Фришман, И.** Детский оздоровительный лагерь как воспитательная система [Текст] / И. Фришман // Народное образование. – 2006. – № 3. – С. 77–81.

3 Антология педагогической мысли Казахстана [Текст] : научное издание / сост. К. Б. Жарикбаев, сост. С. К. Калиев. – Алматы : Рауан, 1995. – 512 с. : ил. – ISBN 5625027587.

Место работы автора (-ов):

Международный Казахско-Турецкий университет имени Х. А. Яссави, г. Туркестан.

А. Б. Есімова

Отбасылық-туысты қатынастар репродуктивті мінез-құлықты жүзеге асырудағы әлеуметтік капитал ретінде

Қ. А. Ясауи атындағы Халықаралық қазақ-түрік университеті, Түркістан қ.

A. B. Yessimova

The family-related networks as social capital for realization of reproductive behaviors

K. A. Yssawi International Kazakh-Turkish University, Turkestan.

Бұл мақалада автор Қазақстандағы әйелдердің отбасылық-туыстық қатынасы арқылы репродуктивті мінез-құлықында айырмашылықтарын талдайды.

In the given article the author analyzes distinctions of reproductive behavior of married women of Kazakhstan through the prism of the kinship networks.

Теруге 24.06.2013 ж. жіберілді. Басуға 29.06.2013 ж. қол қойылды.
Форматы 70х100 1/16. Кітап-журнал қағазы.
Көлемі шартты 5,1 б.т. Таралымы 300 дана. Бағасы келісім бойынша.
Компьютерде беттеген М. А. Шрейдер
Корректорлар: Б. Б. Әубакірова, А. Елемескызы, А. Р. Омарова
Тапсырыс № 2109

Сдано в набор 24.06.2013 г. Подписано в печать 29.06.2013 г.
Формат 70х100 1/16. Бумага книжно-журнальная.
Объем 5,1 ч.-изд. л. Тираж 300 экз. Цена договорная.
Компьютерная верстка М. А. Шрейдер
Корректоры: Б. Б. Аубакирова, А. Елемескызы, А. Р. Омарова
Заказ № 2109

«КЕРЕКУ» баспасы
С. Торайғыров атындағы
Павлодар мемлекеттік университеті
140008, Павлодар қ., Ломов к., 64, 137 каб.
67-36-69
E-mail: publish@psu.kz
kereky@mail.ru