

ДОБУВАННЯ КВАДРАТНОГО КОРЕНЯ З ЕЛЕМЕНТА СКІНЧЕНОЇ ГРУПИ

Іванов І.А.

Науковий керівник – Барковська А. А.

Однією з основних структур сучасної математики є групи. Важливо зазначити, що формалізація такого кардинального поняття як симетрія (в широкому сенсі цього слова), яке присутнє в усіх природничих науках, приводить до поняття групи симетрії. Тому застосування теорії груп є одним з основних методів сучасної теоретичної фізики. Скінченні групи, а також скінченні поля є основним математичним апаратом теорії кодування криптографії – тих прикладних галузей сучасної алгебри, які використовуються для захисту інформації.

В даній доповіді ми розглядаємо скінченні групи, зокрема скінченні симетричні групи – тобто групи усіх перестановок скінченної множини відносно звичайної операції суперпозиції бінарних відношень. Слід зазначити, що з відомої теореми Келі випливає, що всі скінченні групи вичерпуються підгрупами симетричних груп. Саме тому симетричні групи відіграють особливу роль в теорії груп. Нами розроблені програми для знаходження суперпозиції двох перестановок, а також обчислення порядку перестановки. Крім того вивчалася операція добування квадратного кореня з елемента скінченної групи. Знайдено умови при яких ця операція є однозначною. Доведено, що рівняння $x^2 = a$ може і не мати розв'язків. При доведенні останнього твердження ми суттєво використовували поняття циклічної групи – тобто групи яка породжується одним елементом. Крім того у наших викладках застосовується класична теорема Лагранжа, яка говорить про те, що кількість елементів підгрупи скінченної групи є дільником порядку самої групи.

Рівняння $x^2 = a$ розглядалося також на скінченній напівгрупі. Доведено, що вищезгадане рівняння для будь-якого елемента a напівгрупи S має, причому єдиний розв'язок, тоді і тільки тоді, коли напівгрупа S є об'єднання груп, кожна з яких непарного порядку. При доведенні останньої теореми ми скористалися відомим результатом С. Шварта (1956р.) проте, що скінченна напівгрупа є об'єднанням груп тоді і лише тоді, коли вона є сепаративною, тобто для будь-яких елементів x і y виконується імплікація: $x^2 = xy = y^2 \rightarrow x = y$. Треба зазначити, що доведені теореми не виконуються, якщо група або напівгрупа є нескінченною.