

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Механіко-математичний факультет
Кафедра алгебри, топології та основ математики

Затверджено

На засіданні кафедри алгебри,
топології та основ математики
механіко-математичного
факультету
Львівського національного
університету імені Івана Франка
(протокол № __1__ від __01.09. 2020 р.)

Завідувач кафедри алгебри,
топології та основ математики

проф. Зарічний М.М.

**Силабус з навчальної дисципліни
«АЛГЕБРА ТА ТЕОРІЯ ЧИСЕЛ»,
що викладається в межах ОПП (ОПН)
першого (бакалаврського) рівня вищої освіти
для здобувачів зі спеціальності 111 «Математика»**

Львів – 2020

Назва дисципліни	Алгебра і теорія чисел
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, механіко-математичний факультет, м. Львів, вул. Університетська, 1, 79000
Факультет та кафедра, за якою закріплена дисципліна	Механіко-математичний факультет, кафедра алгебри, топології та основ математики
Галузь знань, шифр та назва спеціальності	11 Математика та статистика, 111 «Математика»
Викладачі дисципліни	Романів Олег Миколайович, кандидат фізико-математичних наук, доцент, доцент кафедри алгебри, топології та основ математики; Мельник Іванна Орестівна, кандидат фізико-математичних наук, доцент, доцент кафедри алгебри, топології та основ математики;
Контактна інформація викладачів	Роб. тел. (032) 239 41 72 e-mail: oleh.romaniv@lnu.edu.ua , ivanna.melnyk@lnu.edu.ua , м. Львів, вул. Університетська, 1, ауд. 375.
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій або практичних занять (за попередньою домовленістю). Можливі консультації онлайн через Telegram, а також в Zoom (за попередньою домовленістю). Для погодження часу консультацій слід писати на електронну пошту викладача.
Сторінка дисципліни	http://e-learning.lnu.edu.ua/course/view.php?id=3342
Інформація про дисципліну	Дисципліна «Алгебра і теорія чисел» є нормативною дисципліною зі спеціальності 111 «Математика» для освітньої програми першого (бакалаврського) рівня вищої освіти, яка викладається в третьому семестрі в обсязі 3,5 кредити (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Вивчення дисципліни «Алгебра і теорія чисел» необхідне для засвоєння матеріалу пов'язаних з нею дисциплін, які будуть викладатись на курсах, а також дозволить майбутнім фахівцям використовувати набуті знання в своїй професійній діяльності. Саме тому у курсі розглядаються основні алгебраїчні структури (групи, кільця, поля) та елементарна теорія чисел. Даний курс є фундаментальним курсом для математичних спеціальностей і базовим для вивчення таких дисциплін як «Прикладна алгебра»,

	«Математичні основи захисту інформації», «Основи криптографії».
Мета та цілі дисципліни	<p>Метою дисципліни «Алгебра і теорія чисел» є ознайомлення та оволодіння сучасними методами, теоретичними положеннями та основними застосуваннями абстрактної алгебри та теорії чисел в різних задачах математики, економіки, програмування, комп’ютерних наук, криптографії тощо.</p> <p>Завдання дисципліни: вивчення базових понять абстрактної алгебри та теорії чисел, підготовка до використання набутих знань в подальших навчальних курсах, сприяння розвитку логічного та аналітичного мислення студентів.</p>
Література для вивчення дисципліни	<p style="text-align: center;">Основна</p> <ol style="list-style-type: none"> 1. <i>Андрійчук В. І., Забавський Б. В.</i> Алгебра і теорія чисел. – Львів: ЛНУ ім. І. Франка, 2009. – 266 с. 1. <i>Завало С.Т., Костарчук В.Н., Хацет Б.И.</i> Алгебра і теорія чисел. Ч.2. – К.: Вища школа, 1976. – 384 с. 2. <i>Бухштаб А.А.</i> Теория чисел. – М.:Просвещение, 1966. – 384 с. 3. Алгебра і теорія чисел. Практикум. Ч. 2 / С.Т. Завало, С.С. Левіщенко, В.В. Пилаєв, І.О. Рокицький. – К.: Вища школа, 1986. – 264 с. <p style="text-align: center;">Додаткова</p> <ol style="list-style-type: none"> 1. <i>Завало С.Т.</i> Курс алгебри. – К.: Вища школа, 1985. – 503 с. 2. <i>Виноградов И.М.</i> Основы теории чисел. – М.: Наука, 1981. – 176 с. 3. <i>Бородін О.І.</i> Теорія чисел. – К.: Вища школа, 1970. – 275 с. 4. <i>Кострикін А.І.</i> Введение в алгебру. Ч. III. Основные структуры. – 3-е изд. – М.: ФИЗМАТЛИТ, 2004. – 272 с. 5. <i>Кострикін А.І.</i> Введение в алгебру. – М.: Наука, 1977. – 496 с. 6. <i>Ван дер Варден Б. Л.</i> Алгебра. – М.: Наука, 1976. – 624 с. 7. <i>Ленг С.</i> Алгебра. – М.: Мир, 1968. – 564 с. 8. Навчально-методичний посібник з алгебри і теорії чисел / Уклад. О.Л. Горбачук, М.Я. Комарницький, Ю.П. Матурін. – Львів: Видавничий центр ЛНУ ім. І.Франка, 2006. – 106 с. 9. Сборник задач по алгебре / Под ред А.И. Кострикина. – М.: Физматлит, 2001. – 464 с. 10. <i>Прокуряков И. В.</i> Сборник задач по лінійній алгебре. – 7-е изд. – М.: Наука, 1984. – 336 с.

	<i>11. Винберг Э.Б. Курс алгебры. – М.: Факториал Пресс, 2002. – 544 с.</i>
Обсяг дисципліни	64 години аудиторних занять. З них 32 години лекцій, 32 години практичних занять та 64 години самостійної роботи.
Очікувані результати навчання	<p>Після завершення курсу «Алгебра і теорія чисел» студент буде:</p> <p>знати: основні поняття абстрактної алгебри і теорії чисел, зокрема: група, підгрупа, кільце, поле, скінченне поле, розширення поля, степінь розширення поля, характеристика поля, поле розкладу многочлена, алгебраїчне, трансцендентне число, мінімальний многочлен, просте число, основна теорема арифметики, теореми Ферма, Ейлера, Вільсона, ланцюговий дріб, конгруенція в кільці цілих чисел, квадратичний лишок та нелишок, символ Лежандра, квадратичний закон взаємності.</p> <p>вміти: будувати прості розширення полів, знаходити степінь розширення, виконувати арифметичні дії у скінченних розширеннях полів, будувати поле розкладу многочлена, перевіряти, чи є заданий елемент алгебраїчним та знаходити мінімальний многочлен, будувати скінченні поля, перетворювати конгруенції у еквівалентні, розкладати дійсне число в ланцюговий дріб, застосувати алгоритм Евкліда для знаходження НСД цілих чисел, знаходити кількість і суму всіх дільників числа, значення функції Ейлера, застосовувати ланцюгові дроби до знаходження раціонального наближення дійсних чисел, розв'язувати лінійні конгруенції з одним невідомим та їх системи, розв'язувати лінійні діофантові рівняння з використанням конгруенцій та ланцюгових дробів, перевіряти, чи буде задане число квадратичним лишком за модулем n, знаходити значення символу Лежандра.</p>
Ключові слова	Група, підгрупа, кільце, поле, розширення поля, степінь розширення поля, характеристика поля, поле розкладу многочлена, алгебраїчне, трансцендентне число, мінімальний многочлен, просте число, основна теорема арифметики, теорема Ферма, теорема Ейлера, ланцюговий дріб, конгруенція в кільці цілих чисел, квадратичний лишок, символ Лежандра, символ Якобі, квадратичний закон взаємності.
Формат дисципліни	Очний
	Проведення лекцій, практичних занять та консультацій для кращого розуміння тем.

Теми	Курс складається з двох змістових модулів.					
------	--	--	--	--	--	--

Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Денна форма					
	Усього	у тому числі				
		л	п	лаб	інд	ср
1	2	3	4	5	6	7

Змістовий модуль 1. Елементи абстрактної алгебри

Тема 1. Основи теорії груп	16	4	4			8
Тема 2. Основи теорії кілець	16	4	4			8
Тема 3. Основи теорії полів	8	2	2			4
Колоквіум 1	8	2	2			4
Разом – змістовий модуль 1	24	12	12			12

Змістовий модуль 2. Елементарна теорія чисел

Тема 4. Подільність в кільці цілих чисел	8	2	2			4
Тема 5. Основні функції в теорії чисел	4	1	1			2
Тема 6. Ланцюгові дроби	16	4	4			8
Тема 7. Конгруенції в кільці цілих чисел. Кільця класів лишків	8	2	2			4
Тема 8. Конгруенції першого степеня та їх системи	16	4	4			8
Тема 9. Конгруенції вищих степенів	24	6	6			12
Тема 10. Степеневі лишки. Первісні корені та індекси	4	1	1			2
Колоквіум 2	4	2				2
Контрольна робота	4		2			2

Разом – змістовий модуль 2	96	24	24			48
Усього годин	128	32	32			64
Підсумковий контроль, форма	Іспит у письмовій формі.					
Пререквізити	Для вивчення дисципліни студенти потребують базових знань зі курсів «Лінійна алгебра», «Математичний аналіз», «Дискретна математика».					
Постреквізити	Дисципліна є базовою для вивчення таких дисциплін як «Прикладна алгебра», «Математичні основи захисту інформації», «Захист інформації», «Основи криптографії», «Теоретико-числові алгоритми криптографії».					
Навчальні методи та техніки, які будуть використовуватися під час викладання дисципліни	Лекції, виконання практичних завдань, консультації.					
Необхідне обладнання	Мультимедійний центр для презентацій.					
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Результати навчальної діяльності студентів в семестрі оцінюються за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: Контрольні роботи (лабораторні заняття): 25% семестрової оцінки; максимальна кількість балів 25. Колоквіуми (теоретична частина курсу): 25% семестрової оцінки; максимальна кількість балів 25. Іспит: 50% семестрової оцінки. Максимальна кількість балів 50.					
Політика курсу	<p><i>Академічна добросердість.</i> Очікується, що студенти виконуватимуть навчальні завдання, завдання поточного та підсумкового контролю самостійно, не користуються недозволеними засобами, не видають за свої результати роботи інших людей. При використанні чужих ідей і тверджень у власних роботах посилаються на використані джерела інформації.</p> <p><i>Виявлення ознак академічної недобросердісті</i> в письмовій роботі студента є підставою для її незарахування викладачем.</p> <p><i>Відвідування занять.</i> Очікується, що всі студенти відвідають усі лекції та лабораторні заняття дисципліни. За згоди декана та викладача дозволяється перейти на індивідуальний графік занять. У будь-якому випадку студенти зобов'язані дотримуватися термінів виконання усіх видів робіт, передбачених робочою програмою</p>					

	курсу.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано після завершення курсу.
Питання до екзамену	<p>1. Групи та підгрупи.</p> <p>2. Підгрупи. Критерій підгрупи. Циклічні підгрупи і групи.</p> <p>3. Суміжні класи групи за підгрупою та їх властивості.</p> <p>4. Теорема Лагранжа та її наслідки.</p> <p>5. Нормальні підгрупи.</p> <p>6. Фактор-групи.</p> <p>7. Ізоморфізми груп.</p> <p>8. Ізоморфізми циклічних і скінченних груп</p> <p>9. Гомоморфізми груп.</p> <p>10.Дія групи на множині</p> <p>11.Теореми Силова.</p> <p>12.Прямі добутки і прямі суми груп</p> <p>13.Скінченні абелеві групи та їх розклад в пряму суму. Розклад циклічних груп у пряму суму.</p> <p>14.Кільця і підкільця.</p> <p>15.Операції над ідеалами.</p> <p>16.Головні та скінченно породжені ідеали.</p> <p>17.Кільця головних ідеалів.</p> <p>18.Фактор-кільця.</p> <p>19.Гомоморфізми кілець. Властивості. Ядро і образ гомоморфізму.</p> <p>20.Основна теорема про гомоморфізм кілець.</p> <p>21.Ізоморфізми кілець.</p> <p>22.Поле і підполе. Розширення полів. Характеристика поля. Класифікація полів.</p> <p>23.Примітивні елементи і степені розширень.</p> <p>24.Алгебраїчні і трансцендентні числа.</p> <p>25.Теорема Кронекера-Артіна.</p> <p>26.Поле розкладу многочлена.</p> <p>27.Скінченні поля. Мультиплікативна група скінченного поля.</p> <p>28.Відношення подільності, його найпростіші властивості. Теорема про ділення з остачею.</p> <p>29.Прості і складені числа. Теорема Евкліда.</p> <p>30.Канонічний розклад натурального числа (основна теорема арифметики).</p> <p>31.Найбільший спільний дільник та найменше спільне кратне цілих чисел. Алгоритм Евкліда.</p> <p>32.Властивості НСД. Лінійне зображення НСД.</p> <p>33.Взаємно прості числа.</p>

	<p>34. Числові функції. Ціла і дробова частини дійсного числа.</p> <p>35. Кількість та сума натуральних дільників.</p> <p>36. Функція Ейлера.</p> <p>37. Ланцюгові дроби. Зображення раціональних чисел ланцюговими дробами.</p> <p>38. Підхідні дроби. Рекурентні формули для обчислення чисельника і знаменника підхідного дробу.</p> <p>39. Властивості підхідних дробів.</p> <p>40. Застосування ланцюгових дробів до розв'язування невизначених (діофантових) рівнянь.</p> <p>41. Нескінченні ланцюгові дроби.</p> <p>42. Конгруенції в кільці цілих чисел та їх найпростіші властивості.</p> <p>43. Теореми Ейлера і Ферма.</p> <p>44. Конгруенції першого степеня з одним невідомим: існування розв'язків, методи розв'язування.</p> <p>45. Системи конгруенцій першого степеня з одним невідомим.</p> <p>46. Конгруенції n-го степеня за простим модулем з одним невідомим: побудова еквівалентних конгруенцій.</p> <p>47. Двочленні конгруенції другого степеня. Квадратичні лишки і немешки. Критерій Ейлера.</p> <p>48. Символ Лежандра, його властивості. Квадратичний закон взаємності.</p> <p>49. Символ Якобі.</p> <p>50. Застосування конгруенцій до розв'язування діофантових рівнянь.</p> <p>51. Показники за даним модулем. Первісні корені за простим модулем. Індекси.</p>
--	--