СОФИЙСКИ УНИВЕРСИТЕТ "СВ. КЛ. ОХРИДСКИ"

ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА

КОНСПЕКТ ПО ВИСША АЛГЕБРА

Специалност Информатика, I курс,
учебната 2012-2013 г.

1. Делимост на цели числа. Сравнения.
2. Групи. Теорема на Кейли.
3. Циклични групи.
4. Съседни класове. Теорема на Лагранж. Следствия. Теореми на Ойлер-Ферма и Уилсън.
5. Нормални подгрупи. Факторгрупи. Теорема за хомоморфизмите.
6. Действие на група върху множество. Крайни групи от симетрии. (Вж. също [6].)
7. Идея за криптография. Приложение на теорията на числата в криптоситемите с публичен ключ. (Вж. [5, 7, 8].)
8. Пръстени и полета. Характеристика на поле. Прости полета. Влагане на област на цялост в поле от частни.
9. Идеали. Факторпръстени. Теорема за хомоморфизмите. Китайска теорема за остатъците.
10. Полиноми на една променлива. Алгоритъм за деление с остатък.
11. Аритметика в пръстена на полиномите над поле.
12. Корени на полиномите. Формули на Виет. Кратни корени.
13. Полиноми на няколко променливи. Симетрични полиноми.
14. Дискриминанта и резултанта.
15. Полиноми с комплексни и с реални коефициенти. Алгебрическа затвореност на полето на комплексните числа.
16. Полиноми с рационални коефициенти. Критерии за неразложимост.
17. Крайни полета.
18. Идея за теория на кодирането, коригиращо грешки. .(Вж. [9, 10, 11].)

Основна литература:

1. П. Сидеров, Записки по алгебра (групи, пръстени, полиноми), Веди, София 2006.
2. А. Божилов, П. Сидеров, К. Чакърян, Задачи по алгебра (групи, пръстени, полиноми), Веди, София 2002.

Допълнителна литература:

3. К. Дочев, Д. Димитров, В. Чуканов, Ръководство за упражнения по висша алгебра (пръстени и полета, полиноми, групи), Наука и изкуство, 1976.
4. Г. Генов, С. Миховски, Т. Моллов, Алгебра с теория на числата, Наука и изкуство, 1991.
5. Н. Манев, Увод в теорията на числата, http://manev.net/edu/NumbTh.html.
6. А. Кострикин, Въведение в алгебрата, София 1981.
7. Public-key cryptography.
8. RSA (algorithm).
9. Жак Вофман, Еварист Галоа и планетата Марс: Увод в алгебричната теория на кодирането, Физико-математическо списание, 30, 1988, № 2, 104-116.
10. Идея за теория на кодирането.
11. Великова-Бандова Е., Двоични шумозащитни кодове, ФОИ-Комерс, София, 2004.

Акад. В. Дренски