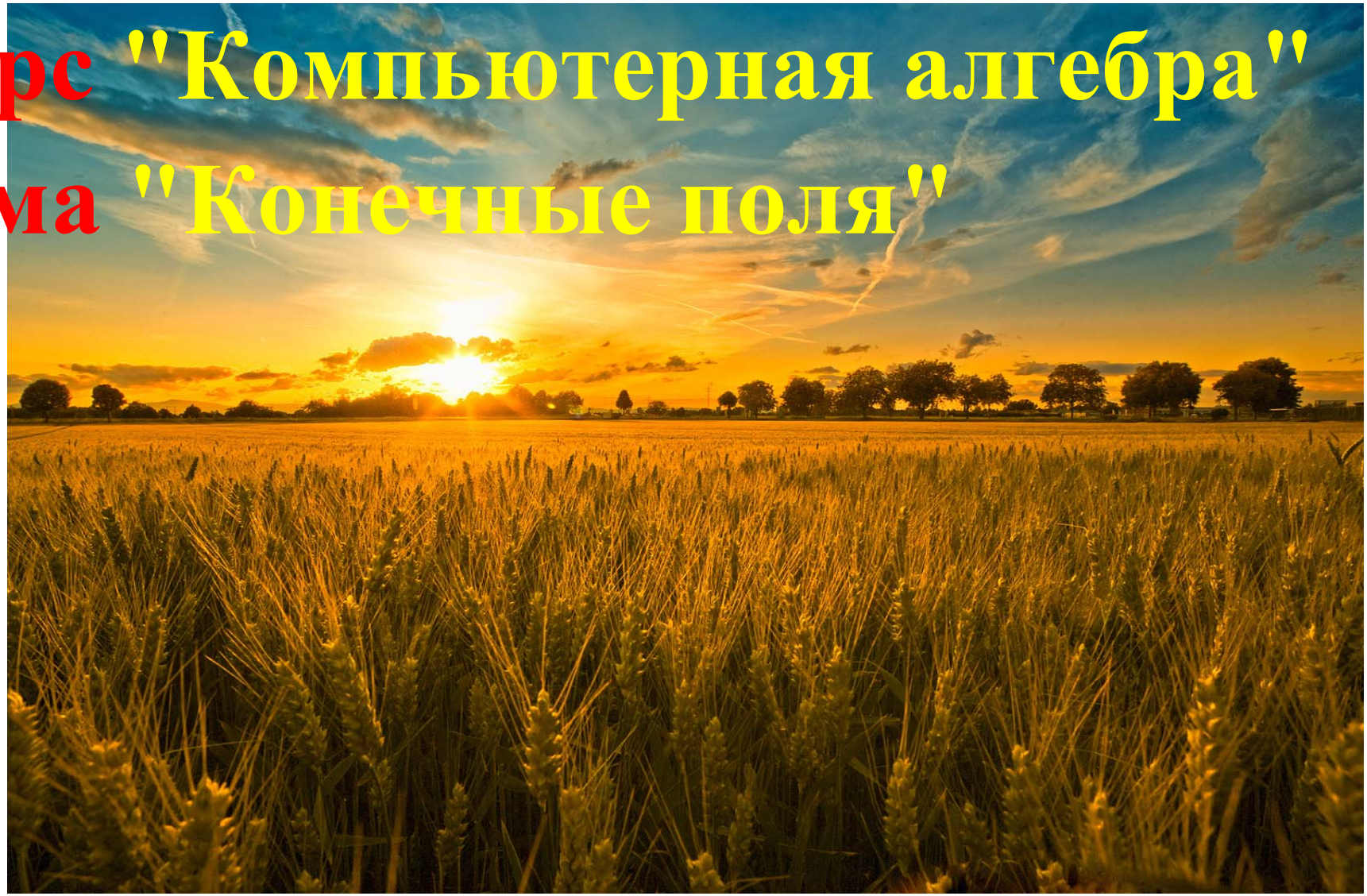
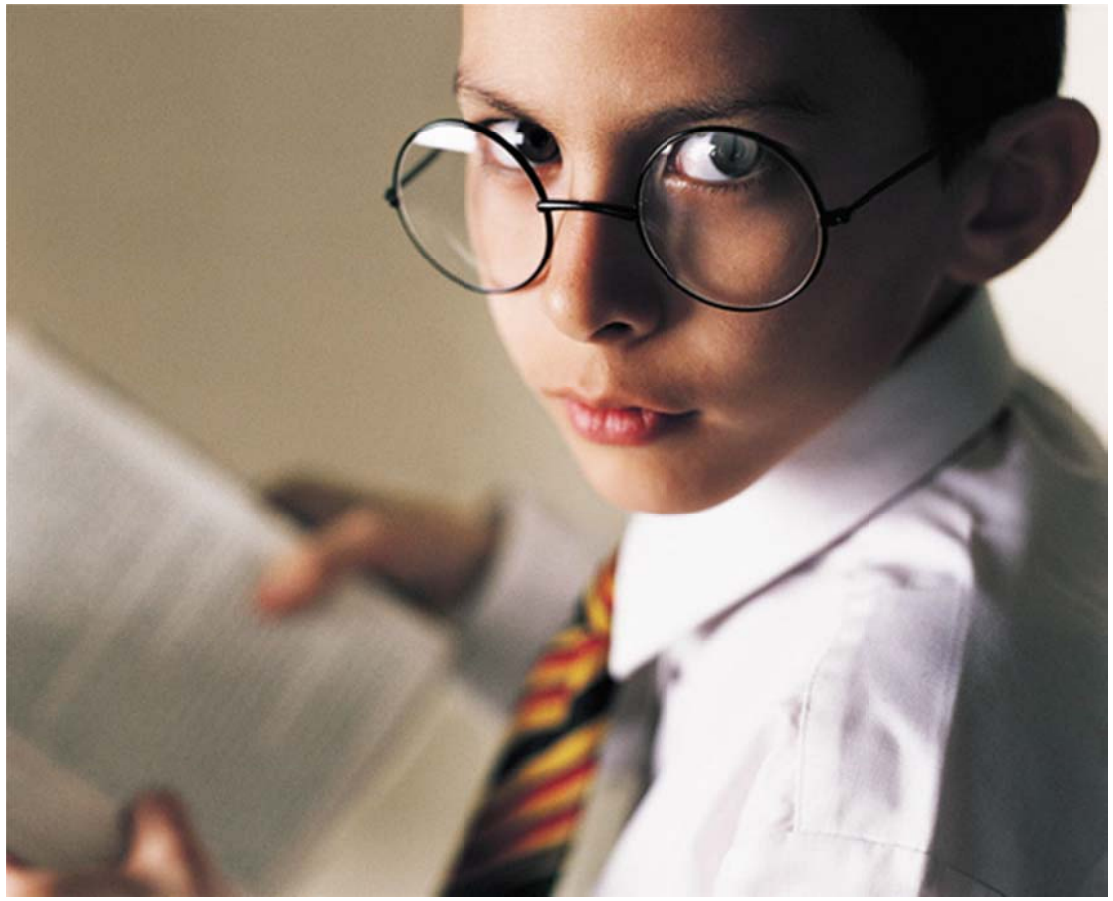
Курс "Компьютерная алгебра"

Тема "Конечные поля"





Школьная алгебра живет и работает в ***поле действительных чисел*** **R**.

Поле – это множество, на котором заданы две алгебраические операции, ***сложение*** и ***умножение***, удовлетворяющие девяти ***аксиомам***: переместительные, сочетательные и распределительные законы; существование противоположных и обратных элементов и т. п.

Поле действительных чисел ***бесконечно***.

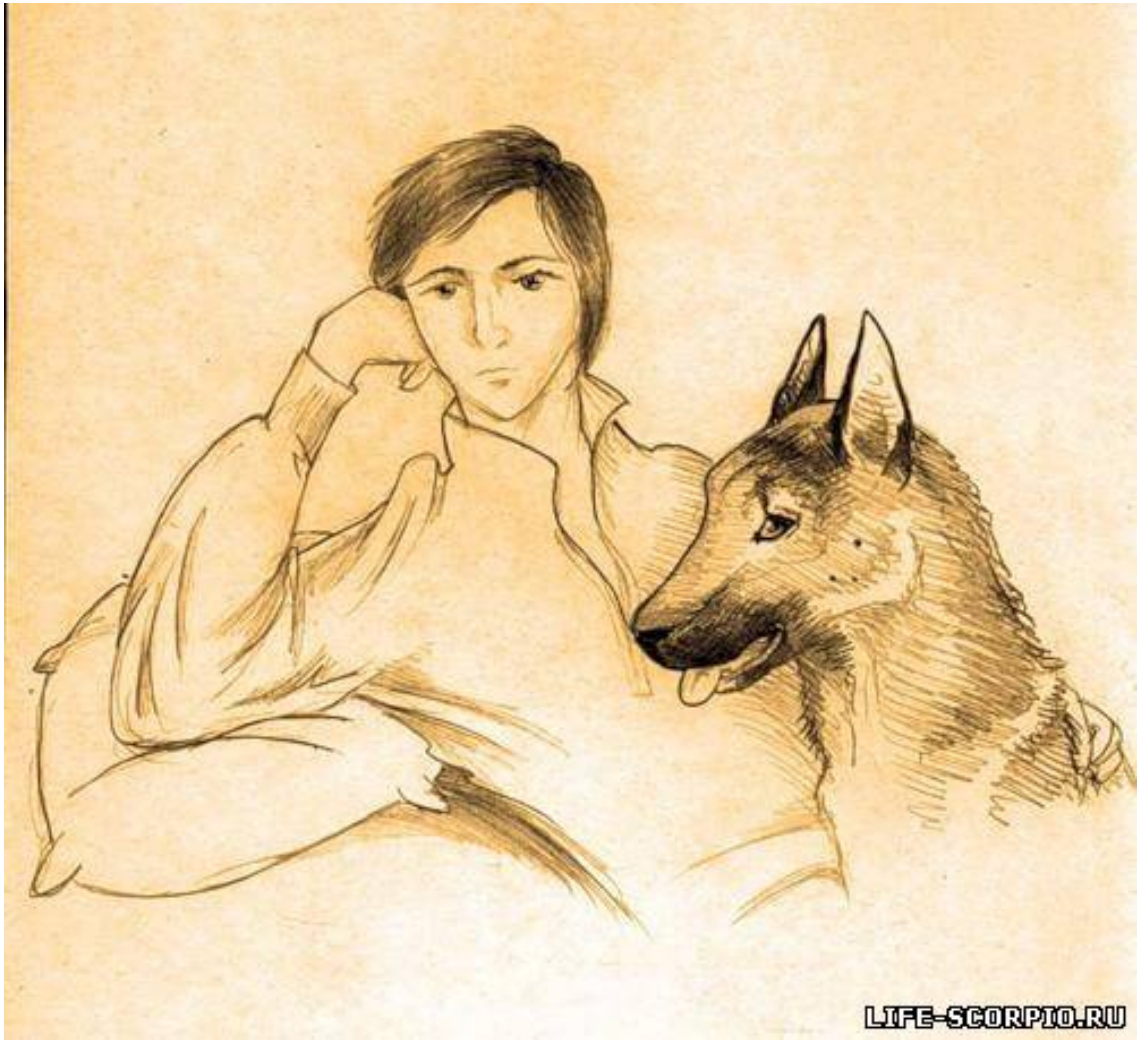
Существуют (и представляют значительный интерес в вопросах ***защиты информации*** и практической ***криптографии***) ***конечные поля (поля Галуа)***.

Самое простое поле F_2 содержит всего два элемента, **0** и **1**, алгебраические действия над которыми - "почти обычные", с единственным исключением:

$$1 + 1 = 0.$$

Таблица сложения:

+	0	1
0	0	1
1	1	0



Поле $F_3 = \{0, 1, 2\}$ также очень легко описать: все действия выполнятся ***по модулю 3***, т. е. выполнив сложение или умножение, надо еще вычислить ***остаток*** от деления полученного результата на **3**.

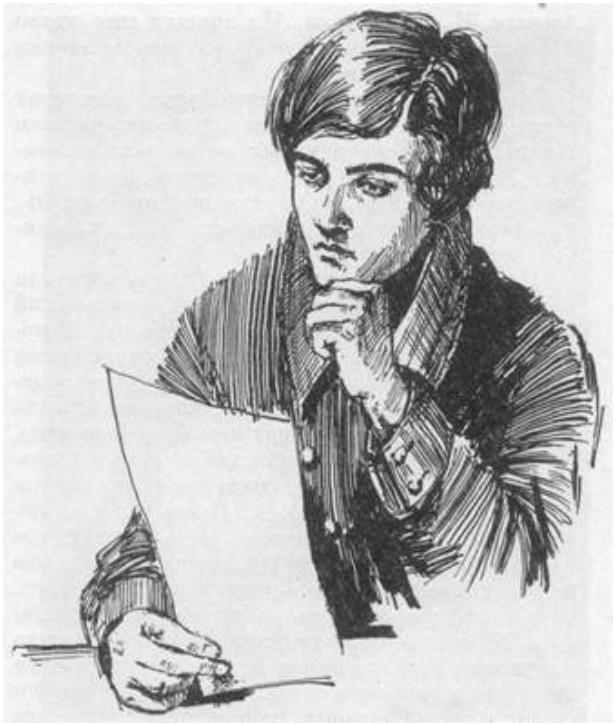
Таблица умножения:

*	0	1	2
0	0	0	0
1	1	1	2
2	2	2	1

Дважды два = 1.

Аналогично устроены другие ***простые поля*** $\mathbf{F}_p$, количество элементов p в каждом из них должно быть ***простым натуральным числом***.

Более сложным (но и более интересным) является описание произвольных конечных полей $\mathbf{F}_q$. Количество элементов в поле $\mathbf{F}_q$ обязано быть ***примарным числом***, т. е. степенью простого числа: $q = p^n$.



Чтобы задать поле $\mathbf{F_8}$ из восьми элементов ($\mathbf{8=2^3}$) надо прежде всего найти ***неприводимый*** многочлен $\boldsymbol{f(x)}$ степени **3** с коэффициентами из $\mathbf{F_2}$. ("Неприводимый" – это значит: ***не разлагается в произведение двух многочленов меньшей степени***.)

Многочлен $\boldsymbol{f(x) = x^3 + x + 1}$ будет именно таким. Далее рассматривается множество многочленов с коэффициентами из $\mathbf{F_2}$, имеющих степень, ***меньшую, чем*** **3**. Их как раз восемь: $\mathbf{F_8 = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}}$.

Эти многочлены можно складывать и умножать обычным образом (не забывая про таблицы сложения и умножения для коэффициентов). Если результат какого-либо действия имеет степень, большую двух, то он должен быть ***приведен по модулю многочлена*** $f(x)$, т. е. заменен на ***остаток*** от деления на $f(x)$.

См. далее (полученные с помощью компьютерной алгебраической системы **Maple**) таблицы сложения и умножения.

Табл. 1. Сложение в F_8.

+	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

Обратите внимание: сумма каждого элемента с самим собой равна нулю; например: $x + x = 0$.

Табл. 2. Умножение в F_8.

*	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Обратите внимание: для каждого ненулевого элемента поля из таблицы 2 усматривается обратный элемент; например: $x^{-1} = x^2 + 1$.

Эвари́ст Галуа́
(фр. ***Évariste Galois***; **1811 — 1832**) — выдающийся французский математик, один из первооткрывателей теории ***групп*** и ***полей***. Радикальный революционер-республиканец, он был застрелен на дуэли в возрасте двадцати лет.
В ночь перед дуэлью Галуа подготовил мемуар для Академии, где кратко изложил итоги своих исследований. Наиболее известный результат Галуа: необходимое и достаточное условие для того, чтобы ***корни алгебраического уравнения допускали выражение через радикалы***. Но наиболее ценным был даже не этот результат, а те ***методы***, с помощью которых Галуа удалось его получить.