АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ НАД РАСШИРЕНИЯМИ ПОЛЕЙ

1 Операции в кольцах и полях над расширениями полей

Будем иметь в виду некоторое конечное поле $F_p = GF(p)$, характеристики p, его расширение $F_{p^m} = GF(p^m)$, замыкание $\overline{F}_p$ и использовать общее обозначение K для этих полей. Над любым из них можно строить полиномы, совокупность K[X] которых является кольцом. Пусть $f(X)$ – многочлен такого кольца. Тогда множество вычетов по модулю $f(X)$ (т.е. остатков отделения многочленов из $K[X]$ на многочлен $f(X)$) также является кольцом и обозначается $K[X]_{f(X)}$, а если при этом многочлен $f(X)$ неприводим и имеет степень k, то кольцо $K[X]_{f(X)}$ является полем и в случае, когда $K = GF(p^m)$, обозначается $GF(p^{m^k})$. При $m > 1$ кольца $GF(p^m)[X]$, $GF(p^m)_{f(X)}$ и поля $GF(p^{m^k})$ являются алгебраическими структурами над расширением $GF(p^m)$ простого поля $GF(p)$. Над полем $GF(p^{m^k})$ можно также определить эллиптические кривые $EC(GF(p^{m^k}))$.

Операции в кольцах $K[X]$. Операция сложения в кольце $K[X]$ выполняется сложением в поле K коэффициентов многочленов при одинаковых степенях переменной. Операция умножения в кольце $K[X]$ определяется как обычно, при этом умножение коэффициентов осуществляется по правилам умножения в поле K, элементами, которого они являются, при $k > 1$ и использовании полиномиального базиса такая операция включает умножение в кольце $GF(p)[X]$ с приведением по модулю неприводимого многочлена $q(X)$, степени k корнем которого порождается базис поля $K = GF(p^k)$.

Пример 1.1 Вычисление в кольце $K[X] = GF(2^2)[X]$ суммы и произведения двух полиномов степени 2 над полем $K = GF(2^2)$, заданных векторами коэффициентов при степенях переменной в порядке их возрастания

$\alpha_1 =$ (11,01,10);
$\alpha_2 =$ (10,11,01);

приведено в табл. 1.6 а), б). В данном случае многочлен $q(X) = 1 + X + X^2$.

Операции в поле $GF(p^{k^m})$ **над полем** $GF(p^k)$**.** Допустим $n = mk$, НОД$(m, k) = 1$ и представим поле $GF(p^n)$ как расширение степени k поля $GF(p^m)$: $GF(p^n) = GF((p^m)^k) = GF(p^m)(\lambda)$, где $\lambda \in GF(p^n),\ \lambda \notin GF(p^m)$.

Пример 1.2 $p = 2,\ ,m = 2,\ k = 3$. $GF(2^n) = GF(2^6) = GF(2^2)(\lambda)$, *где* $\lambda \in GF(2^6),\ \lambda \notin GF(2^2)$.

Можно показать, что неприводимый многочлен $p(X)$ степени k над полем $GF(p)$ является также неприводимым многочленом над полем $GF(p^m)$ (идея доказательства: алгоритм тестирования на неприводимость многочленов над $GF(p)$ и над $GF(p^n)$ будет иметь одинаковые исходы каждой итерации, так как коэффициенты многочлена над $GF(p^m)$ принадлежат полю $GF(p)$). При этом степени

$$1,\ \lambda,\ \ldots,\ \lambda^{k-1} \tag{1}$$

его корня λ составляют базис подполя $GF(p^k)$ поля $GF(p^m)^k$. Аналогично неприводимый многочлен $q(X)$ степени m над $GF(p)$ является неприводимым многочленом над полем $GF(p^m)$, и степени

$$1,\ \mu,\ldots,\ \mu^{m-1} \tag{2}$$

его корня μ образуют базис подполя $GF(2^m)$ поля $GF(p^m)^k$. Произведение базисов (1) и (2) (km) векторов образует базис K поля $GF((2^m)^k)$:

$$1,\ \lambda,\ \ldots,\ \lambda^{k-1},\ \mu, \lambda\mu,\ \ldots,\ \lambda^{k-1}\mu, \ldots, \mu^{k-1}\ \lambda\mu^{m-1}, \ldots, \lambda^{k-1}\mu^{m-1} \tag{3}$$

Элементы α поля $GF(2^n)$ представляются как k-местные векторы, компонентами которых являются m-местные векторы из элементов поля $GF(p)$:

$$((a_{0\ 0}, \ldots, a_{0\ m-1}), \ldots, (a_{k-1\ 0}, \ldots, a_{k-1\ m-1})). \tag{4}$$

Векторы-коэффициенты $(a_{j-1\ 0}, \ldots, a_{j-1\ m-1}),\ j = 1, \ldots k$ суть векторы коэффициентов представления элементов поля $GF(p^m)$ в стандартном базисе этого поля, порождаемом корнем μ некоторого известного неприводимого многочлена $q(X)$ степени m. В свою очередь, эти векторы являются коэффициентами представления элементов поля $GF(2^m)(\lambda)$ в стандартном базисе, порождаемом корнем λ также известного неприводимого многочлена $p(X)$ степени k над полем $GF(p^m)$ (этот многочлен можно выбрать как неприводимый многочлен степени k над полем $GF(p)$.

Если в представлении (4) опустить внутренние скобки и запятые, то получится представление этого же элемента поля $GF(p^{mk})$ в базисе (3).

Пример 1.3 $p = 2$, $m = 2$, $k = 3$. $GF((p^m)^k)$=$GF(p^k)(\lambda) = GF(p)(\mu)(\lambda)$. Присоединяя к $GF(2)$ корень $\mu = (01)$ многочлена $1 + X + X^2$, получаем поле $GF(2)(\mu) = \{00, 01, 10, 11\}$. Далее присоединяя корень $\lambda = (00, 10, 00)$ многочлена $1 + X^2 + X^3$ (это корень 010 того же многочлена над $GF(2)$) получаем поле $GF(p^k)(\lambda) = \{(00, 00, 00), \ldots, (11, 11, 11)\}$. Пример элемента такого поля: $\alpha = (11, 01, 10) = (1 + \mu) + (\mu)\lambda + 1 \cdot \lambda^2$.

Так устроенное поле $GF(2^m)(\lambda)$ условимся называется *композитным полем.*

Операция сложения элементов композитного поля это операция поразрядного сложения соответствующих друг другу векторов.

Пример 1.4 Пример вычисления суммы двух элементов дан в табл. 1.6 а).

Алгоритм умножения в поле $GF(p^m)(\lambda)$ включает два этапа – умножение в кольце $GF(2^m)[X]$ и последующее редуцирование – приведение по модулю неприводимого многочлена $p(X)$.

Пример 1.5 Редуцируем результат умножения в кольце из предыдущего примера по модулю многочлена $p(X) = 1 + X^2 + X^3$:

$$\begin{array}{llllll}
(11 & 00 & 10 & 00 & 01)+ \\
(& 01 & 00 & 01 & 01)+ \\
\hline
(11 & 01 & 10 & 01 &)+ \\
(01 & 00 & 01 & 01 &)= \\
\hline
(10 & 01 & 11 & &).
\end{array}$$

Пример 1.6 Пусть $m = 3$, $k = 2$, и поле $GF(2^3)$ порождается многочленом $p(X) = 1 + X + X^3$. Возьмем неприводимый многочлен $q(X) = 1 + X + X^2$ над $GF(2)$ и будем использовать соответствующий неприводимый многочлен $1 + X + X^2$ над полем $GF(2^3)$ (его коэффициенты принадлежат как $GF(2)$, так и $GF(2^3)$). Элементы $(100, 000)$, $\mu = (010, 000)$, $\mu^2 = (001, 000)$ где $\mu = (010, 000)$ – корень многочлена $p(X)$ образуют базис подполя $GF(2^3)$. Элементы $(100, 000), \lambda = (000, 100)$ образуют базис подполя $GF(2^2)$ поля $GF((2^3)^2)$.

Шесть элементов базиса поля $GF((2^3)^2)$ следующие: $(100, 000)$, $\mu = (010, 000)$, $\mu^2 = (001, 000)$, $\lambda = (000, 100)$, $\lambda\mu = (000, 010)$, $\lambda\mu^2 = (000, 001)$. В явном виде такой базис в вычислениях не используется.

Некоторые степени элемента $\alpha = (000, 010)$ даны в табл. 1.6 в).

Таблица 1: а) Сложение в кольце $GF(2^2)[X]$ и в поле $GF((2^2)^3)$; б) умножение в кольце $GF(2^2)[X]$; в) некоторые степени образующего элемента группы $GF((2^3)^2)^*$, г) некоторые степени элемента $(5,6)$ группы $GF(7^2)^*$, д) возведение в квадрат элемента $(5,6)$ поля $GF(7^2)$, е) возведение в квадрат элемента $(15,25)$ поля $GF(127^2)$

а)

$\alpha_1=$	(11,01,10);
$\alpha_2=$	(10,11,10);
$\alpha_1 \ +\alpha_2 =$	
$\alpha_1 + \alpha_2 =$	(01,10,00).

б) $\alpha_1 \times \alpha_2 =$

(11× 10	01× 10	10× 10	0	0)+
(0	11× 11	01× 11	10× 11	0)+
(0	0	11× 01	01× 01	10× 01)=
(11	01	10	0	0) +
(0	01	10	11	0)+
(0	0	10	11	01)=
(11	00	10	00	01).

в)

$\alpha =$	$(000,010)$	$\alpha^2 =$	$(001,001)$
$\alpha^4 =$	$(000,011)$	$\alpha^8 =$	$(010,010)$
$\alpha^{16} =$	$(000,001)$	$\alpha^{32} =$	$(011,011)$
$\alpha^{48} =$	$(101,000)$	$\alpha^{56} =$	$(100,100)$
$\alpha^{60} =$	$(011,000)$	$\alpha^{62} =$	$(101,101) = \alpha^{-1}$
$\alpha^{63} =$	$(100,000) = 1$		
$\alpha^{64} =$	$(000,010)$		

г)

$\alpha =$	$(5,6)$	$\alpha^2 =$	$(3,4)$
$\alpha^4 =$	$(0,3)$	$\alpha^8 =$	$(5,0)$
$\alpha^{16} =$	$(4,0)$	$\alpha^{24} =$	$(6,0)$
$\alpha^{32} =$	$(2,0)$	$\alpha^{40} =$	$(3,0)$
$\alpha^{44} =$	$(0,2)$	$\alpha^{46} =$	$(6,6)$
$\alpha^{47} =$	$(1,3) = \alpha^{-1}$	$\alpha^{48} =$	$(1,0)$

д)			е)		
5	6		15	25	
×			×		
5	6	=	19	30	=
4	2		31	94	+
+				69	115=
	2	1=	31	36	115=
4	4	1=	31	36	
4	4	+	+		
6		=	12		=
3	4		43	36	

Операции в квадратичном расширении поля $GF(p)$. Теперь рассмотрим операцию умножения в поле $GF(p^2)$ – квадратичном расширении поля $GF(p)$. Полиномиальный базис этого поля составляют элементы 1=(1,0) и $\lambda = (0,1)$. Здесь λ есть корень неприводимого многочлена $a_0 + a_1X + X^2$, где $a_0, a_1 \in GF(p)$. В частности, можно взять $a_1 = 0$, тогда $-a_0$ есть квадратичный невычет по модулю p.

Заметим, что если $p \equiv 3 \bmod 4$, то число $p-1 \equiv -1 \bmod p$ есть квадратичный невычет, и $X^2-(p-1) = X^2+1$ неприводим в $GF(p^2)$.

Пример 1.7 Пусть $m = 1$, $k = 2$, $p = 7$. Возведем $5+6X \in GF(7^2)$ в степень $7^2-1 = 48$ в поле $GF(3^2)$, порождаемом неприводимым многочленом X^2+1 (заметим, что $6 \equiv -1 \bmod 7$ есть квадратичный невычет).

Элементы $(0,0), (1,0)$, $(2,0)$, $(3,0)$, $(4,0)$, $(5,0)$, $(6,0)$ образуют подполе $GF(7)$, его базис есть элемент $(1,0)$. Элементы $(1,0)$, $(0,1)$ составляют базис поля $GF(7^2)$.

Вычислим некоторые степени элемента $(5,6)$ (см. табл. 1.6 г).

Элемент (5,6) является примитивным элементом поля $GF(p^2)$, так как

$$\begin{aligned} \alpha^{16} = &\quad (4,0) \neq (1,0), \\ \alpha^{24} = &\quad (6,0) \neq (1,0). \end{aligned}$$

В табл. 1.6 д) и е) приведены вычисления при возведении в квадрат элементов полей $GF(7^2)$ и $GF(127^2)$.

2 Структура мультипликативной группы $GF(q^k)^*$.

Обозначим $\mu_n \subset \overline{GF(q)}\ ^*$ подгруппу всех корней n-й степени из единицы. На самом деле эта подгруппа содержится уже в конечном подполе $GF(q^k)$ поля $\overline{K}$, где k — мультипликативный порядок числа q по модулю n, т.е. наименьшее такое k, что q^k-1 кратно n, и не содержится в полях меньшего порядка. Действительно, если в поле $GF(q^m)$ есть элемент x, такой, что $x^n = 1$, то его мультипликативная группа, имеющая порядок q^m-1, содержит подгруппу порядка n, состоящую из элементов $\{1, x, x^2, \ldots, x^{n-1}\}$, и по теореме Лагранжа о подгруппах q^m-1 делится на n, откуда $m \geq k$. В тоже время в поле $GF(q^k)$ в качестве x можно выбрать $g^{(q^k-1)/n}$, где g — примитивный элемент поля, тогда $x^n = g^{q^k-1} = 1$, и группа корней n-й степени из единицы есть $\{1, x, x^2, \ldots, x^{n-1}\}$.

Так определяемое число k называется *множителем безопасности* или *степенью вложения.*

Пример 2.1 Мультипликативным порядком числа 19 по модулю 5 является число 2: $19^2 - 1 = 360$, кратное 5, в то время, как число $19 - 1 = 18$ на 5 не делится. Рассмотрим поле $GF(19^2)$, порождаемое неприводимым многочленом $X^2 + 1$. Порядок его мультипликативной группы есть 360. Элемент $(3, 2)$ является примитивным элементом этого поля. Корень 5-ой степени из единицы получается возведением примитивного элемента в степень $\frac{p^2-1}{n}$: $(3, 2)^{72} = (2, 15)$.

Упражнение 2.1 Напишите алгоритм определения мультипликативного порядка числа и перечисления всех корней n-ой степени из единицы.

Далее будет использоваться фактор группа $GF(q^k)^*/GF(q^k)^{*n}$ по подгруппе $GF(q^k)^{*n}$. [1] Образующий элемент (порядка $\frac{q^k-1}{n}$) этой подгруппы можно получить возведением в степень n примитивного элемента поля. Применительно к только что рассмотренному примеру таким элементом будет $(3, 2)^5 = (11, 8)$. Далее возведением этого элемента в соответствующие степени получаются остальные элементы подгруппы (всего получим 72 элемента). Элементы смежных классов по этой подгруппе можно последовательно получить, умножая все элементы группы на определенный элемент группы корней n-ой степени из единицы.

Пример 2.2 Мультипликативным порядком числа 11 по модулю 3 является число 2: $11^2 - 1 = 120$, кратное 3, в то время, как число $11 - 1 = 10$ на 3 не делится. Рассмотрим поле $GF(11^2)$, порождаемое неприводимым многочленом $X^2 + 1$ Порядок его мультипликативной группы есть 120. Элемент $(2, 3)$ является примитивным элементом этого поля. Корень 3-ой степени из единицы получается возведением примитивного элемента в степень $\frac{p^2-1}{n}$: $(2, 3)^{40} = (5, 8)$.

Группа корней 3-ой степени из 1 есть

$$\mu_3 = \{(5, 8), (5, 3), (1, 0)\}.$$

Вычислим образующий элемент группы $GF(11^2)^3$, для этого возведем образующий элемент группы $GF(11^2)$ в куб:

$$(2, 3)^3 = (9, 9).$$

[1]Такое обозначение соответствует тому, что элементы подгруппы получаются возведением в степень n элементов группы.

Вычислим последовательно элементы подгруппы $GF(11^2)^3$:

$$GF(11^2)^3 = \{(9,9),(0,8),(5,6),(2,0),(7,7),(0,5),(10,1),(4,0),(3,3),
(0,10),(9,2),(8,0),(6,6),(0,9),(7,4),(5,0),(1,1),(0,7),(3,8),(10,0),
(2,2),(0,3),(6,5),(9,0),(4,4),(0,6),(1,10),(7,0),(8,8),(0,1),(2,9),
(3,0),(5,5),(0,2),(4,7),(6,0),(10,10),(0,4),(8,3),(\mathbf{1},\mathbf{0})\}. \tag{5}$$

Остальные два смежных класса по этой подгруппе получим умножением ее элементов на элементы $(5,8)$ и $(5,3)$ подгруппы μ_3 :

$$(5,8)\times GF(11^2)^3 = \{(6,7),(2,7),(10,4),(10,5),(1,3),(4,3),(9,8),
(9,10),(2,6),(8,6),(7,5),(7,9),(4,1),(5,1),(3,10),(3,7),(8,2),(10,2),
(6,9),(6,3),(5,4),(9,4),(1,7),(1,6),(10,8),(7,8),(2,3),(2,10,(9,5),
(3,5),(4,6),(4,2),(7,10),(6,10),(8,1),(8,4),(3,9),(1,9),(5,2),(\mathbf{5},\mathbf{8}); \tag{2}$$

$$(5,3)\times GF(11^2)^3 = \{(7,6),(9,7),(7,1),(10,6),(3,1),(7,3),(3,2),
(9,1),(6,2),(3,6),(6,4),(7,2),(1,4),(6,1),(1,8),(3,4),(2,8),(1,2),
(2,5),(6,8),(4,5),(2,4),(4,10),(1,5),(8,10),(4,8),(8,9),(2,10),(5,9),
(8,5),(5,7),(4,9),(10,7),(5,10),(10,3),(8,7),(9,3),(10,9),(9,6),(\mathbf{5},\mathbf{3})\}. \tag{-1}$$

Обратим внимание, что каждый класс смежности по подгруппе $GF(p^2)^n$ содержит единственный элемент группы μ_n и каждый элемент класса преобразуется в этот элемент при возведении в степень $\frac{p^2-1}{n}$.

Пример 2.3 В продолжение предыдущего примера имеем $(9,9)^{\frac{11^2-1}{3}} = (9,9)^{40} = (0,8)^{40} = \cdots = (1,0)$; $(6,7)^{\frac{11^2-1}{3}} = (6,7)^{40} = (2,7)^{40} = \cdots = (5,8)$; $(7,6)^{\frac{11^2-1}{3}} = (7,6)^{40} = (9,7)^{40} = \cdots = (5,3)$;

Упражнение 2.2 В продолжение примера **??** вычислите элементы группы $GF(2^{3^4})^{*5}$ и четыре других смежных класса по этой подгруппе группы $GF(2^{3^2})^*$.

Упражнение 2.3 Напишите алгоритм порождения подгруппы $GF(q^k)^n,\ q = pq = 2^m,\ q = 3^m$, и вычисления всех смежных классов. Обратите внимание, что фактор группа $GF(q^k)^n$ изоморфна группе μ_n.

3 Группа точек n-кручения эллиптической кривой.

Пусть E — эллиптическая кривая над полем $K = GF(q)$ и n — число, взаимно простое с характеристикой поля. Обозначим $\overline{K}$ алгебраическое замыкание этого поля. Рассмотрим кривую $E(\overline{K})$. Точку P этой кривой назовем *точкой кручения порядка* n (или просто n-кручения), если $nP = \underbrace{P + \ldots + P}_{n} = \mathcal{O}$ в группе точек кривой. Множество точек n-кручения кривой $E(\overline{K})$ обозначим $E[n]$. Несложно проверить, что $E[n]$ замкнуто относительно сложения точек и поэтому образует подгруппу в группе кривой $E(\overline{K})$. На самом деле она является подгруппой группы кривой $(GF(q^k))$ над некоторым конечным расширением поля $GF(q)$. Здесь k – тот же множитель безопасности (степень вложения), который выше был определен применительно к мультипликативной группе поля $GF(p)$. Подгруппу $E(n)$ будем обозначать также $hE(GF(p^k))$, где $h = \frac{q^k-1}{n}$, подчеркивая тот факт, что эта подгруппа может быть получена умножением каждой точки эллиптической кривой $E(GF(p^k))$ на константу h.

Известна весьма нетривиальная теорема о том, что группа $E[n]$ изоморфна прямой сумме двух циклических групп порядка n, короче, $E[n] \sim Z_n \oplus Z_n$. Прямая сумма двух аддитивных групп $G \oplus H$ определяется как множество всех упорядоченных пар $(g, h), g \in G, h \in H$, на котором операция сложения определяется покомпонентно, т.е. $(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2)$. Нетрудно проверить, что прямая сумма двух групп тоже будет группой с нулевым элементом $(0, 0)$ и порядком, равным произведению порядков слагаемых. В частности, порядок $E[n]$ равен n^2. Если порядки слагаемых циклических групп взаимно просты, то и их сумма будет циклической группой, но в рассматриваемом случае это не так, и группа $E[n]$ не циклическая, так как порядок каждого ее элемента равен n (но она содержит циклические подгруппы порядка n).

Алгоритм вычисления множества $E[n] = hE(GF(p^2))$

Входом являются характеристика p поля, неприводимый многочлен $X^2 + NQR$ над $GF(p)$ и коэффициенты a и b уравнения кривой $EC : Y^2 = X^3 + aX + b$ над полем $GF(p)$, выходом - все циклические подгруппы множества $E[n] = hEC(GF(p^2))$.

Найти точку $P \in EC(GF(p))$ порядка n и точку $P' \in EC'(GF(p))$ порядка n, где $EC' : Y^2 = X^3 + NQR^2aX + NGR^3b$ – скрученная кривая.

Перевести точку $P = (x, y)$ в формат $extP = ((x, 0), (y, 0))$ элемента группы $P \in EC(GF(p^2))$, и присвоить $P = extP$; точку $P' = (x', y')$ также перевести в формат $extP' = ((x', 0), (y', 0))$; далее применить гомоморфизм Ψ для получения точки $Q = \Psi P' = ((-x', 0), (0, y')) \in E(GF(p^2))$, неколлинеарной точке P.

Для $j = 1, n$,
$U = P$,
$E(1, j) = U$,
$U = U + P$,
$U = P + Q$,
для $i = 2, n + 1$,
$V = U$;
для $j = 1, n$
$E(i, j) = V$,
$V = V + U$,
$U = U + P$.

Заметим,что этот алгоритм приведен здесь для иллюстрации структуры группы кручения и практически не применяется, так как при больших n практически не реализуем.

Заметим,что этот алгоритм приведен здесь для иллюстрации структуры группы кручения и практически не применяется, так как при больших n практически не реализуем.

Пример 3.1 Группа n-кручения эллиптической кривой $Y^2 = X^3 - 3X$ над полем $GF(11^2)$, $(n = 3)$ состоит из 4-х циклических подгрупп:

$$\begin{pmatrix} \begin{matrix}9&0\\8&0\end{matrix} & \begin{matrix}9&0\\3&0\end{matrix} & \mathcal{O} \\ \begin{matrix}0&3\\2&2\end{matrix} & \begin{matrix}0&3\\9&9\end{matrix} & \mathcal{O} \\ \begin{matrix}0&8\\9&2\end{matrix} & \begin{matrix}0&8\\2&9\end{matrix} & \mathcal{O} \\ \begin{matrix}2&0\\0&8\end{matrix} & \begin{matrix}2&0\\0&3\end{matrix} & \mathcal{O} \end{pmatrix} \tag{0}$$

Упражнение 3.1 Напишите алгоритмы вычисления прямой суммы $Z_n \oplus Z_n$, где n – простое и приведите пример.

Указание. Нетрудно видеть его подобие алгоритму вычисления множества $E[n]$.

Группа $nE(GF(p^k))$ и фактор группа $E(GF(p^k))/nE(GF(p^k))$. Элементы группы $nE(GF(p^k))$ получаются умножением элементов группы $E(GF(p^k))$ на n. После этого классы смежности фактор группы $E(GF(p^k))/nE(GF(p^k))$ получаются прибавлением определённых элементов группы кручения $E[n]$ к элементам группы $nE(GF(p^k))$.

Всего получится n^2 смежных классов и каждый из них содержит точно один элемент группы $E[n]$. По построению, фактор группа $E(GF(p^k))/nE(GF(p^k))$ изоморфна группе кручения $E[n]$.

Пример 3.2 Группа кручения $E[3]$ кривой $y^2 = X^3 - 3X$ над $GF(11^2)$ содержит 4 подгруппы порядка 3 (см. (0)).

Группа $3E(GF(11^2))$, получающаяся умножением на константу $n = 3$ точек группы точек эллиптической кривой $Y^2 = X^3 - 3X$ над полем $GF(11^2)$, содержит 16 точек :

$$\begin{pmatrix} \mathcal{O} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 5 \\ 2 & 9 \end{pmatrix} & \begin{pmatrix} 0 & 5 \\ 9 & 2 \end{pmatrix} \\ \begin{pmatrix} 0 & 6 \\ 2 & 2 \end{pmatrix} & \begin{pmatrix} 0 & 6 \\ 9 & 9 \end{pmatrix} & \begin{pmatrix} 5 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 5 & 4 \\ 4 & 6 \end{pmatrix} \\ \begin{pmatrix} 5 & 4 \\ 7 & 5 \end{pmatrix} & \begin{pmatrix} 5 & 7 \\ 4 & 5 \end{pmatrix} & \begin{pmatrix} 5 & 7 \\ 7 & 6 \end{pmatrix} & \begin{pmatrix} 6 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 6 & 4 \\ 5 & 7 \end{pmatrix} & \begin{pmatrix} 6 & 4 \\ 6 & 4 \end{pmatrix} & \begin{pmatrix} 6 & 7 \\ 5 & 4 \end{pmatrix} & \begin{pmatrix} 6 & 7 \\ 6 & 7 \end{pmatrix} \end{pmatrix} \tag{1}$$

Прибавлением к каждой точке этой группы некоторой отличной от $\mathcal{O}$ точки группы 3-кручения (0) получим дополнительно еще 8 смежных классов:

$$\begin{pmatrix} \begin{pmatrix} \mathbf{9} & \mathbf{0} \\ \mathbf{8} & \mathbf{0} \end{pmatrix} & \begin{pmatrix} 7 & 0 \\ 6 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 6 \\ 8 & 3 \end{pmatrix} & \begin{pmatrix} 2 & 10 \\ 1 & 7 \end{pmatrix} \\ \begin{pmatrix} 1 & 5 \\ 8 & 8 \end{pmatrix} & \begin{pmatrix} 2 & 1 \\ 1 & 4 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 8 & 0 \end{pmatrix} & \begin{pmatrix} 4 & 5 \\ 8 & 9 \end{pmatrix} \\ \begin{pmatrix} 9 & 9 \\ 4 & 7 \end{pmatrix} & \begin{pmatrix} 4 & 6 \\ 8 & 2 \end{pmatrix} & \begin{pmatrix} 9 & 2 \\ 4 & 4 \end{pmatrix} & \begin{pmatrix} 8 & 0 \\ 2 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 10 \\ 2 & 3 \end{pmatrix} & \begin{pmatrix} 4 & 7 \\ 1 & 8 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 2 & 8 \end{pmatrix} & \begin{pmatrix} 4 & 4 \\ 1 & 3 \end{pmatrix} \end{pmatrix} \tag{2}$$

$$\begin{pmatrix} \begin{pmatrix} \mathbf{9} & \mathbf{0} \\ \mathbf{3} & \mathbf{0} \end{pmatrix} & \begin{pmatrix} 7 & 0 \\ 5 & 0 \end{pmatrix} & \begin{pmatrix} 2 & 10 \\ 10 & 4 \end{pmatrix} & \begin{pmatrix} 1 & 6 \\ 3 & 8 \end{pmatrix} \\ \begin{pmatrix} 2 & 1 \\ 10 & 7 \end{pmatrix} & \begin{pmatrix} 1 & 5 \\ 3 & 3 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 3 & 0 \end{pmatrix} & \begin{pmatrix} 9 & 9 \\ 7 & 4 \end{pmatrix} \\ \begin{pmatrix} 4 & 5 \\ 3 & 2 \end{pmatrix} & \begin{pmatrix} 9 & 2 \\ 7 & 7 \end{pmatrix} & \begin{pmatrix} 4 & 6 \\ 3 & 9 \end{pmatrix} & \begin{pmatrix} 8 & 0 \\ 9 & 0 \end{pmatrix} \\ \begin{pmatrix} 4 & 7 \\ 10 & 3 \end{pmatrix} & \begin{pmatrix} 1 & 10 \\ 9 & 8 \end{pmatrix} & \begin{pmatrix} 4 & 4 \\ 10 & 8 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 9 & 3 \end{pmatrix} \end{pmatrix} \tag{3}$$

$$\begin{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{3} \\ \mathbf{2} & \mathbf{2} \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 3 & 3 \end{pmatrix} & \begin{pmatrix} 4 & 3 \\ 6 & 9 \end{pmatrix} & \begin{pmatrix} 7 & 3 \\ 9 & 6 \end{pmatrix} \\ \begin{pmatrix} 0 & 2 \\ 9 & 9 \end{pmatrix} & \begin{pmatrix} 0 & 7 \\ 7 & 7 \end{pmatrix} & \begin{pmatrix} 8 & 4 \\ 3 & 9 \end{pmatrix} & \begin{pmatrix} 9 & 8 \\ 0 & 6 \end{pmatrix} \\ \begin{pmatrix} 2 & 6 \\ 8 & 5 \end{pmatrix} & \begin{pmatrix} 3 & 1 \\ 10 & 5 \end{pmatrix} & \begin{pmatrix} 7 & 1 \\ 2 & 0 \end{pmatrix} & \begin{pmatrix} 3 & 4 \\ 9 & 3 \end{pmatrix} \\ \begin{pmatrix} 9 & 6 \\ 5 & 8 \end{pmatrix} & \begin{pmatrix} 2 & 8 \\ 6 & 0 \end{pmatrix} & \begin{pmatrix} 8 & 1 \\ 5 & 10 \end{pmatrix} & \begin{pmatrix} 4 & 1 \\ 0 & 2 \end{pmatrix} \end{pmatrix} \tag{4}$$

$$\begin{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{3} \\ \mathbf{9} & \mathbf{9} \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 8 & 8 \end{pmatrix} & \begin{pmatrix} 7 & 3 \\ 2 & 5 \end{pmatrix} & \begin{pmatrix} 4 & 3 \\ 5 & 2 \end{pmatrix} \\ \begin{pmatrix} 0 & 7 \\ 4 & 4 \end{pmatrix} & \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} & \begin{pmatrix} 8 & 4 \\ 8 & 2 \end{pmatrix} & \begin{pmatrix} 2 & 6 \\ 3 & 6 \end{pmatrix} \\ \begin{pmatrix} 9 & 8 \\ 0 & 5 \end{pmatrix} & \begin{pmatrix} 7 & 1 \\ 9 & 0 \end{pmatrix} & \begin{pmatrix} 3 & 1 \\ 1 & 6 \end{pmatrix} & \begin{pmatrix} 3 & 4 \\ 2 & 8 \end{pmatrix} \\ \begin{pmatrix} 2 & 8 \\ 5 & 0 \end{pmatrix} & \begin{pmatrix} 9 & 6 \\ 6 & 3 \end{pmatrix} & \begin{pmatrix} 4 & 1 \\ 0 & 9 \end{pmatrix} & \begin{pmatrix} 8 & 1 \\ 6 & 1 \end{pmatrix} \end{pmatrix} \tag{5}$$

$$\begin{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{8} \\ \mathbf{9} & \mathbf{2} \end{pmatrix} & \begin{pmatrix} 0 & 10 \\ 8 & 3 \end{pmatrix} & \begin{pmatrix} 0 & 4 \\ 4 & 7 \end{pmatrix} & \begin{pmatrix} 0 & 9 \\ 2 & 9 \end{pmatrix} \\ \begin{pmatrix} 7 & 8 \\ 2 & 6 \end{pmatrix} & \begin{pmatrix} 4 & 8 \\ 5 & 9 \end{pmatrix} & \begin{pmatrix} 8 & 7 \\ 8 & 9 \end{pmatrix} & \begin{pmatrix} 7 & 10 \\ 9 & 0 \end{pmatrix} \\ \begin{pmatrix} 3 & 10 \\ 1 & 5 \end{pmatrix} & \begin{pmatrix} 2 & 5 \\ 3 & 5 \end{pmatrix} & \begin{pmatrix} 9 & 3 \\ 0 & 6 \end{pmatrix} & \begin{pmatrix} 3 & 7 \\ 2 & 3 \end{pmatrix} \\ \begin{pmatrix} 4 & 10 \\ 0 & 2 \end{pmatrix} & \begin{pmatrix} 8 & 10 \\ 6 & 10 \end{pmatrix} & \begin{pmatrix} 2 & 3 \\ 5 & 0 \end{pmatrix} & \begin{pmatrix} 9 & 5 \\ 6 & 8 \end{pmatrix} \end{pmatrix} \tag{6}$$

$$\begin{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{8} \\ \mathbf{2} & \mathbf{9} \end{pmatrix} & \begin{pmatrix} 0 & 10 \\ 3 & 8 \end{pmatrix} & \begin{pmatrix} 0 & 9 \\ 9 & 2 \end{pmatrix} & \begin{pmatrix} 0 & 4 \\ 7 & 4 \end{pmatrix} \\ \begin{pmatrix} 4 & 8 \\ 6 & 2 \end{pmatrix} & \begin{pmatrix} 7 & 8 \\ 9 & 5 \end{pmatrix} & \begin{pmatrix} 8 & 7 \\ 3 & 2 \end{pmatrix} & \begin{pmatrix} 3 & 10 \\ 10 & 6 \end{pmatrix} \\ \begin{pmatrix} 7 & 10 \\ 2 & 0 \end{pmatrix} & \begin{pmatrix} 9 & 3 \\ 0 & 5 \end{pmatrix} & \begin{pmatrix} 2 & 5 \\ 8 & 6 \end{pmatrix} & \begin{pmatrix} 3 & 7 \\ 9 & 8 \end{pmatrix} \\ \begin{pmatrix} 8 & 10 \\ 5 & 1 \end{pmatrix} & \begin{pmatrix} 4 & 10 \\ 0 & 9 \end{pmatrix} & \begin{pmatrix} 9 & 5 \\ 5 & 3 \end{pmatrix} & \begin{pmatrix} 2 & 3 \\ 6 & 0 \end{pmatrix} \end{pmatrix} \tag{7}$$

$$
\begin{pmatrix}
\begin{pmatrix} \mathbf{2} & \mathbf{0} \\ \mathbf{0} & \mathbf{8} \end{pmatrix} & \begin{pmatrix} 4 & 0 \\ 0 & 6 \end{pmatrix} & \begin{pmatrix} 9 & 10 \\ 7 & 1 \end{pmatrix} & \begin{pmatrix} 10 & 6 \\ 3 & 8 \end{pmatrix} \\
\begin{pmatrix} 10 & 5 \\ 8 & 8 \end{pmatrix} & \begin{pmatrix} 9 & 1 \\ 4 & 1 \end{pmatrix} & \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} & \begin{pmatrix} 7 & 7 \\ 8 & 1 \end{pmatrix} \\
\begin{pmatrix} 10 & 10 \\ 3 & 2 \end{pmatrix} & \begin{pmatrix} 10 & 1 \\ 8 & 2 \end{pmatrix} & \begin{pmatrix} 7 & 4 \\ 3 & 1 \end{pmatrix} & \begin{pmatrix} 10 & 0 \\ 0 & 8 \end{pmatrix} \\
\begin{pmatrix} 2 & 9 \\ 7 & 4 \end{pmatrix} & \begin{pmatrix} 7 & 5 \\ 9 & 8 \end{pmatrix} & \begin{pmatrix} 7 & 6 \\ 2 & 8 \end{pmatrix} & \begin{pmatrix} 2 & 2 \\ 4 & 4 \end{pmatrix}
\end{pmatrix} \tag{8}
$$

$$
\begin{pmatrix}
\begin{pmatrix} \mathbf{2} & \mathbf{0} \\ \mathbf{0} & \mathbf{3} \end{pmatrix} & \begin{pmatrix} 4 & 0 \\ 0 & 5 \end{pmatrix} & \begin{pmatrix} 10 & 6 \\ 8 & 3 \end{pmatrix} & \begin{pmatrix} 9 & 10 \\ 4 & 10 \end{pmatrix} \\
\begin{pmatrix} 9 & 1 \\ 7 & 10 \end{pmatrix} & \begin{pmatrix} 10 & 5 \\ 3 & 3 \end{pmatrix} & \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix} & \begin{pmatrix} 10 & 10 \\ 8 & 9 \end{pmatrix} \\
\begin{pmatrix} 7 & 7 \\ 3 & 10 \end{pmatrix} & \begin{pmatrix} 7 & 4 \\ 8 & 10 \end{pmatrix} & \begin{pmatrix} 10 & 1 \\ 3 & 9 \end{pmatrix} & \begin{pmatrix} 10 & 0 \\ 0 & 3 \end{pmatrix} \\
\begin{pmatrix} 7 & 5 \\ 2 & 3 \end{pmatrix} & \begin{pmatrix} 2 & 9 \\ 4 & 7 \end{pmatrix} & \begin{pmatrix} 2 & 2 \\ 7 & 7 \end{pmatrix} & \begin{pmatrix} 7 & 6 \\ 9 & 3 \end{pmatrix}
\end{pmatrix} \tag{9}
$$

Как видим, каждый из 9 смежных классов (1-9)содержит по одной точке группы 3-кручения (0).

Контрольные вопросы

1. Как определяются операции сложения, умножения и деления с остатком в кольцах $GF(2^m)[X]$, $GF(3^m)[X]$ и $GF(p)[X]$?
2. Как определяются операции сложения и умножения в кольцах $GF(2^m)[X]_{f(X)}$, $GF(3^m)[X]_{f(X)}$ и $GF(p)[X]_{f(X)}$?
3. Каким должен быть делитель в операции деления в кольцах $GF(2^m)[X]_{f(X)}$, $GF(3^m)[X]_{f(X)}$ и $GF(p)[X]_{f(X)}$, как эта операция определяется и какими способами может быть реализована?
4. Как определяются и какими способами выполняются операции сложения, умножения и деления в полях $GF(2^{m^k})$, $GF(3^{m6k})$ и $GF(p^k)$?
5. Как найти неприводимые многочлены над полями $GF(2^m)$, $GF(3^n)$, GFp^2?
6. Как определяется в общем виде дивизор ненулевой рациональной функции над кривой?

7. Как определяются мультипликативный порядок числа k по модулю n и подгруппа μ_n всех корней n-ой степени из единицы мультипликативной группы $GF(q^k)$?
8. что такое параметр безопасности, или степень вложения?
9. Как можно сгенерировать все элементы подгруппы $GF(q^k)^n$
10. Как получить смежные классы группы $GF(q^k)$ по подгруппе $GF(q^k)^n$?
11. Как определяется группа n-кручения эллиптической кривой $EC(GF(q^k))$, как получить ее образующий элемент?
12. Как как найти элементы группы $nEC(GF(q^k))$ и затем смежные классы группы $nEC(GF(q^k))$ по этой подгруппе?