2.9.6 Поля

При розгляді кілець було видно, що дільники нуля обмежують використання всіх його елементів. Цього не може статися коли кільце є полем. Поле – це окремий випадок асоціативно-комутативного кільця з одиницею.

Означення 65. *Асоціативно-комутативне кільце з одиницею називається* **полем**, *якщо воно як відносно додавання, так і відносно множення є абелевою групою. Група поля відносно додавання*

називається **адитивною**, *а група відносно множення* – **мультиплікативною**.

Отже, поле є областю цілісності і, як випливає із теореми 53, кільце многочленів над довільним полем P є областю цілісності. Одиницею в цій області цілісності служить многочлен, коефіцієнти якого всі рівні нулю, крім коефіцієнта a_0, який дорівнює 1_P – одиниці поля P.

Поле F називається скінченним, якщо його носій A має скінченне число елементів.

Нехай $a \in F$, тоді елементи $a, a+a, a+a+a, \ldots$ є елементами поля, які будемо позначати $a, 2a, 3a, \ldots, na, \ldots$ відповідно (множник n не обов'язково повинен бути елементом поля F). Аналогічно елементи $a, a \cdot a, a \cdot a \cdot a, \ldots$ теж є елементами поля і їх позначають $a, a^2, a^3, \ldots, a^n, \ldots$ відповідно. Нехай $a \neq 0$ – елемент поля F.

Означення 66. *Якщо існує таке найменше число $n \in \mathcal{N}$, що $n \cdot a = 0$, то n називається адитивним порядком елемента a.*

Якщо існує таке найменше число $n \in \mathcal{N}$, що $a^n = 1$, то n називається мультиплікативним порядком елемента a.

Теорема 58. *Всі ненульові елементи поля F мають один і той же адитивний порядок.*

Доведення. Нехай $a, b \in F \backslash \{0\}$ і їх адитивні порядки дорівнюють n і m відповідно. Тоді

$$n \cdot b = n \cdot (a \cdot a^{-1}) \cdot b = (n \cdot a) \cdot (a^{-1} \cdot b) = 0 \cdot a^{-1} \cdot b = 0.$$

Звідси випливає, що $m \leq n$. Аналогічно

$$m \cdot a = m \cdot (b \cdot b^{-1}) \cdot a = (m \cdot b) \cdot (b^{-1} \cdot a) = 0 \cdot b^{-1} \cdot a = 0.$$

Звідси випливає, що $n \leq m$ і тому $m = n$. ■

Означення 67. *Якщо в полі F всі ненульові елементи мають адитивний порядок n, то поле F називається полем характеристики n. Якщо такого числа n не існує, то поле називається полем характеристики 0.*

Теорема 59. *Характеристика довільного скінченного поля є простим числом.*

Доведення. Нехай F – скінченне поле F і $a \in F \setminus \{0\}$ – довільний його елемент. Тоді в послідовності $a, 2a, 3a, \ldots$ існують такі числа $i, j \in \mathcal{Z}, i < j$, що $ja = ia$ або $(j-i)a = 0$. Отже, поле F має додатну характеристику, яку позначимо n. На підставі того, що поле F включає принаймні два елементи (0 і 1), то $n \geq 2$. Якщо число n не є простим, то існують такі числа $k, l \in \mathcal{Z}, 1 < k, l < n$, що $n = kl$. Тоді

$$0 = n \cdot 1 = (k \cdot l) \cdot 1 = (k \cdot l) \cdot (1 \cdot 1) = (k \cdot 1)(l \cdot 1).$$

Оскільки поле є областю цілісності, то або $k \cdot 1 = 0$ або $l \cdot 1 = 0$. Звідси дістаємо, що або $ka1 = (k1)a = 0$ або $la1 = (l1)a = 0$ для всіх $a \in F$. Але це суперечить означенню характеристики поля n. ■

З доведеної теореми випливає такий основний результат для скінченних полів.

Теорема 60. *Скінченне поле F має характеристику p і порядок p^n для деякого $n \in \mathcal{N}$.*

Доведення. З попередньої теореми випливає, що поле F має характеристику p, де p – просте число. Нехай $|F| = q$. Якщо $q = p$, то твердження теореми, очевидно, має місце. В протилежному випадку візьмемо елемент $a_1 \in F \setminus \{0\}$ і покладемо

$$G_1 = \{y : y = m_1 \cdot a_1,\ m_1 \in \mathcal{N},\ 1 \leq m_1 \leq p\}.$$

Розглянемо тепер елемент $a_2 \in F \setminus G_1$ і побудуємо

$$G_2 = \{z : z = m_1 \cdot a_1 + m_2 \cdot a_2,\ m_1, m_2 \in \mathcal{N},\ 1 \leq m_1, m_2 \leq p\}.$$

Якщо $F \neq G_2$, то розглядається елемент $a_3 \in F \setminus G_2$ і т. д. На підставі скінченності поля F такий процес закінчується і ми отримуємо сукупність множин $G_1, G_2, \ldots, G_n$ для деякого $n \in \mathcal{N}$.

Кожний елемент $a \in F$ єдиним чином представляється у вигляді

$$a = m_1 \cdot a_1 + m_2 \cdot a_2 + \ldots + m_n \cdot a_n,$$

де $1 \leq m_i \leq p$, для всіх $i = 1, 2, \ldots, n$. (Довести це як корисну вправу). Отже, існує p^n таких виразів і тому $|F| = p^n$. ■

Означення 68. *Поле називається простим, якщо воно не має жодного власного підполя.*

Очевидно, що коли поле має простий порядок, то воно є простим полем і порядок простого поля дорівнює характеристиці цього поля. Як випливає з попереднього твердження, простими полями не вичерпуються скінченні поля, оскільки для довільних простого числа p і натурального числа n існує поле порядок якого p^n. Цей більш загальний вигляд скінченних полів будується за допомогою поліномів.

Нехай $F = (A, \Omega)$ – поле. Нагадаємо, що поліномом над полем називається вираз

$$f(x) = \sum_{i=0}^{n} a_i x^i,$$

де $n \in \mathcal{N}$, $a_i \in A$, $0 \leq i \leq n$, а x – символ, який не належить полю F. Коефіцієнт $a_n \neq 0$ називається старшим, якщо $n \neq 0$. Число n називається степенем полінома $f(x)$ і позначається $n = deg(f)$. Якщо старшим коефіцієнтом є a_0, то поліном $f(x)$ називається константою, а коли старший коефіцієнт $a_0 = 0$, то поліном $f(x)$ називається нульовим $f(x) = 0$. Множину всіх поліномів над полем F позначатимемо $F(x)$.

Якщо $f(x), g(x) \in F(x)$, де

$$f(x) = \sum_{i=0}^{n} a_i x^i, \qquad g(x) = \sum_{j=0}^{m} b_j x^j,$$

то

$$f(x) + g(x) = \sum_{k=0}^{\max(m,n)} c_k x^k, \tag{2.48}$$

де

$$c_k = \begin{cases} a_k + b_k, & k = 0, 1, \ldots, \min(m, n), \\ a_k, & k = m+1, \ldots, n, \text{ якщо } m < n, \\ b_k, & k = n+1, \ldots, m, \text{ якщо } n < m. \end{cases}$$

і

$$f(x) \cdot g(x) = \sum_{k=0}^{m+n} c_k x^k, \tag{2.49}$$

де $c_k = \sum\limits_{i+j=k,\ 0 \leq i,j \leq n}^{m+n} a_i b_j.$

Означення 69. *Поліном $f(x) \in F(x)$ називається незвідним над полем F, якщо він має додатний степінь і з рівності $f(x) = g(x) \cdot h(x)$, де $g(x), h(x) \in F(x)$, випливає що або поліном $g(x)$ є константою, або поліном $h(x)$ є константою. В протилежному випадку поліном називається звідним.*

Побудуємо тепер скінченне поле за допомогою незвідного полінома. Зауважимо, що для поліномів $f(x)$ і $g(x)$, де $g(x) \neq 0$ як і при діленні цілих чисел, має місце розклад

$$f(x) = g(x) \cdot h(x) + r(x), \tag{2.50}$$

де $g(x), r(x) \in F(x)$ і $deg(r) < deg(g)$.

Означення 70. *Нехай $f(x), g(x), h(x) \in F(x)$, де $g(x) \neq 0$, задовольняють умові (2.50). Тоді поліном $r(x)$ називається остачею від ділення полінома $f(x)$ на поліном $g(x)$. Цей поліном позначається як $r = f \pmod g$. Остачі від ділення всіх поліномів із множини $F(x)$ за модулем полінома $g(x)$ називаються поліномами із множини $F(x)$ за модулем полінома $g(x)$. Множина всіх таких поліномів позначимо $F_g(x)$.*

Очевидно, що степені всіх поліномів із $F_g(x)$ менші $deg(g)$.

Теорема 61. *Нехай F – поле, а $f(x)$ – ненульовий поліном із $F(x)$. Тоді $F_f(x)$ буде полем тоді і тільки тоді, коли f незвідний над полем $F(x)$.*

Доведення. Спочатку зазначимо, що $F_f(x)$ є кільцем з нулем та одиницею відносно операцій додавання та множення за модулем полінома $f(x)$. Це випливає із співвідношень (2.48), (2.49) і (2.50). Нулем і одиницею виступають 0 і 1 поля F.

Припустимо, що $F_f(x)$ є полем і $f = g \cdot h$, де g і h – поліноми з множини $F(x)$, які не є константами. Тоді, оскільки $0 < deg(g) < deg(f)$ і $0 < deg(h) < deg(f)$, то поліноми g і h не є константами в множині $F_f(x)$, не дивлячись на те, що поліном f є нульовим в полі $F_f(x)$. Але це суперечить замкнутості операції множення в мультиплікативній групі поля $F_f(x)$. Отже, $F_f(x)$ не може бути полем, а це суперечить незвідності полінома $f(x)$ над полем F.

Нехай поліном $f(x)$ незвідний над полем F. Оскільки $F_f(x)$ кільце, то для доведення теореми потрібно показати, що для довільного

ненульового полінома із $F_f(x)$ в ньому існує елемент, обернений відносно операції множення. Нехай r – ненульовий поліном із $F_f(x)$ такий, що НСД$(f, r) = c$. Оскільки $f(x)$ незвідний поліном над полем F і $deg(r) < deg(f)$, то поліном c має бути константою. Розглянемо поліном $h(x) = c \cdot r(x)$, де $c \in F$, $h(x) \in F_f(x)$ і НСД(f, h)=1. До поліномів, як і до цілих чисел, застосовний узагальнений алгоритм Евкліда і знайти $h^{-1}\ (mod\ f) \in F_f(x)$ (деталі алгоритму Евкліда для поліномів можна знайти в [7]). Крім того, оскільки $c \in F$, то існує такий елемент $c^{-1} \in F$, що $r^{-1} = c^{-1} \cdot h^{-1} \in F_f(x)$. ■

Незвідний поліном $f(x)$ називається **визначальним поліномом** поля $F_f(x)$.

Теорема 62. *Нехай F скінченне поле, порядок якого p, де p – просте число, а f – незвідний поліном над полем F степеня n. Тоді $|F_f(x)| = p^n$.*

Доведення. Із означення поля $F_f(x)$ випливає, що множина $F(x)$ складається із поліномів, степінь яких менший $n = deg(f)$, а їх коефіцієнти належать полю F. Але таких поліномів буде p^n. ■

Наслідок 8. *Для кожного простого числа p і кожного $n \in \mathcal{N}$ існує скінченне поле, яке складається із p^n елементів.*

Приклад 2.9.6. 1. Нехай F^2 – поле лишків за модулем 2. Поліном $f(x) = x^2 + x + 1$ є незвідним над полем F^2. Множина $F_f^2(x)$ є полем, яке має 2^2 елементів. Їх степені менші 2 і тому довільний елемент y із цього поля має вигляд:

$$y = b_1 x + b_0,$$

де $b_i \in F^2$, $i = 0, 1$. Таблиці Келі для поля F_2^f приймають вигляд:

$\oplus$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\odot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

2. Одним із важливих прикладів простих полів є скінченні кільця лишків за модулем простого числа p. Це випливає з такої теореми.

Теорема 63. *Кільце лишків Z_p за модулем p буде полем тоді і тільки тоді, коли p просте число.*

Доведення. Для доведення досить встановити існування для кожного $s \in Z_p, s \neq 0$, оберненого елемента $s' \in Z_p$.

Розглянемо елементи $s, 2s, \ldots, (p-1)s$. Всі ці елементи різні і відмінні від нуля, оскільки із $s \neq 0$ випливає $ks \neq 0$ для $k = 1, 2, \ldots, p-1$ на підставі простоти числа

p. А те що вони різні випливає з того, що коли припустити $ks = ls, k < l, l. k < p$, то $(l-k)s = 0$, а це невірно. Отже, послідовність елементів $s, 2s, \ldots, (p-1)s$ збігається з послідовністю переставлених яким-небудь чином елементів $1, 2, \ldots, p-1$. Зокрема, знайдеться $s', 1 \leq s' \leq p-1$, для якого $ss' = 1$, тобто s' – обернений елемент до елемента s.■

Поле Z_p будемо позначати F_p.

Наведемо таблиці Келі поля F_5. Нехай маємо множину $A = \{0, 1, 2, 3, 4\}$, на якій визначені операції додавання і множення за модулем 5. Таблиці Келі для цих операцій матимуть вигляд:

Таблиця 2.9.11

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

,

Таблиця 2.9.12

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

.

Операції додавання і множення задовольняють закони асоціативності і комутативності, а нуль і одиниця є нулем і одиницею цієї алгебри. Крім того, із таблиці множення очевидним чином випливає, що ця алгебра не має дільників нуля, тобто вона є областю цілісності, а, отже, є полем. Очевидно, що побудоване таким способом поле буде простим на підставі простоти модуля p. ♠

З теореми 52 випливає наступна

Теорема 64. *Кожне скінченне просте поле ізоморфне полю лишків F_p [6].*

А з теореми 54 випливає, що всі ненульові елементи мультиплікативної групи поля – дільники одиниці. Таким чином, розгляд простих полів вигляду F_p не обмежує загальності. Звідси випливає, що можна вибирати скінчене просте поле довільним, а не обов'язково полем лишків за модулем простого числа. Враховуючи ізоморфізм між такими полями, це не вносить яких-небудь принципових змін, але може складати додаткові перешкоди для криптоаналітика. Наприклад, в якості простого поля можна взяти поле F, операції якого визначені таблицями додавання (таблиця 2.9.2) і множення (таблиця 2.9.8) (див. стор. 172). Відображення $f(2) = 4, f(3) = 2, f(4) = 3, f(0) = 0, f(1) = 1$ – ізоморфізм між полями F_5 і F.

При перевірці незвідності поліномів користуються *тестом Рабіна* [29], який полягає в наступному.

Нехай $l_1, l_2, \ldots, l_n$ — прості дільники числа k і $k/l_i = m_i$. Поліном $P(x)$ степеня k над полем F_p є незвідним тоді і тільки тоді, коли:

- $P(x)|(x^{p^k} - x)$, тобто $P(x)$ дільник $x^{p^k} - x$,
- $\gcd(P(x), x^{p^{m_i}} - x) = 1$, для всіх $1 \leq i \leq k$,

де скорочення gcd означає НСД.

Приклад 2.9.7. Нехай маємо поліном $P(x) = x^6 + x^5 + 1$ степеня 6 в полі F_2. Ділення полінома $Q(x) = x^{2^6} = x^{64}$ на цей поліном дає в остачі поліном $R(x) = x$, таким чином $P(x)$ задовольняє першій умові тесту Рабіна. Поліноми $x^{2^{6/2}} - x = x^8 - x$ і $x^{2^{6/3}} - x = x^4 - x$ попарно взаємно прості з поліномом $P(x)$, що на підставі тесту Рабіна поліном $x^6 + x^5 + 1$ незвідний в полі F_2.

Якщо розглядається поліном $P(x) = x^2 + x$ степеня 2 в тому ж полі F_2, то остача від ділення полінома $Q(x) = x^{2^2} = x^4$ на цей поліном теж дає в остачі поліном $R(x) = x$. Але, $P(x)$ незвідним не буде, оскільки $x^2 + x = x \cdot (x + 1)$. Дійсно, поліноми $x^{2^{2/2}} - x = x^2 - x$ і $P(x) = x^2 + x$ не є взаємно простими, а тому друга умова тесту Рабіна не виконується. ♠

Зі сказаного випливає такий алгоритм перевірки полінома на незвідність:

```
function is-irreducible(P(x))
begin
  if x^{p^k} ≡ x (mod P(x)) then
    begin
      irreducible = true;
      for l_i in factors(deg(P(x))) do
        begin
          if gcd(P(x), x^{p^{k/l_i}} − x (mod P(x))) ≠ 1 then
            begin
              irreducible = false;
              break;
            end;
        end;
        return irreducible;
      end
  else return false;
end;
```

Тут $\gcd(P(x), q(x))$ – функція обчислення НСД поліномів алгоритмом Евкліда, $\deg(P(x))$ – степінь полинома $P(x)$, а $\text{factors}(n)$ – функція, яка знаходить прості дільники числа n.

Використання в наведеному алгоритмі бінарного піднесення до степеня для обчислення полинома x^{p^k} дає можливість розв'язати порівняння $x^{p^k} \equiv x \ (mod\ P(x))$ і $\gcd(P(x), x^{p^{k/l_i}} - x \ (mod\ P(x))) \neq 1$ за не більш, ніж $2 \cdot \log p^k$ операцій. А використання ефективних

операцій множення і ділення поліномів дозволяє отримати алгоритм, складність якого $O(k^2 \log^2 k \log p \log\log k)$ [29].

Розглянемо ще деякі важливі властивості поля F_q, де $q = p^k$ і p – просте число. Зазначимо, що в полі F_q існує $q-1$ ненульових елементів, які відносно операції множення утворюють абелеву групу. Будемо позначати цю групу F_q^*.

Твердження 6 *Порядок довільного елемента $a \in F_q^*$ є дільником числа q-1.*

Доведення. Нехай d – найменший степінь a, для якого $a^d = 1$. Такий степінь d дійсно існує на підставі скінченності множини F_q^*: різні степені елемента a не можуть бути всі різними і якщо $a^i = a^j, j > i$, то $a^{j-i} = 1$.

Нехай S означає множину $\{1, a, a^2, \ldots, a^{d-1}\}$ всіх різних степенів елемента a. Тоді для довільного $b \in F_q^*$ нехай bS означає клас суміжності, який складається з елементів ba^j (наприклад, $1 \cdot S = S$). Очевидно, що два класи суміжності або збігаються або не мають спільних елементів. Дійсно, якщо $b_1 a^i \in b_1 S$ належить класу $b_2 S$, тобто $b_1 a^i = b_2 a^j$, то для довільного $b_1 a^m$ із $b_1 S$ маємо $b_1 a^m = b_1 a^{i+m-1} = b_2 a^{j+m-i}$. Оскільки кожний клас суміжності складається з d елементів і є розбиттям множини F_q^*, то на підставі теореми Лагранжа $d|q-1$. ■

Означення 71. *Твірним елементом скінченного поля F_q називається елемент g, порядок якого дорівнює q-1, а це еквівалентно тому, що $1, g, g^2, \ldots, g^{q-2}$ є різними елементами F_q^*.*

Теорема 65. *Довільне скінченне поле F_q має твірний елемент. Якщо g – твірний елемент F_q^*, то g^j буде твірним елементом тоді і тільки тоді, коли НСД(j,q-1) = 1. Зокрема, в F_q^* існує $\varphi(q-1)$ різних твірних елементів.*

Доведення. Припустимо, що елемент $a \in F_q^*$ має порядок d, тобто $a^d = 1$ і жодний менший степінь a не дорівнює 1. Тоді на підставі твердження 6 число d дільник $q-1$. Оскільки a^d найменший степінь, який дорівнює 1, то всі елементи $a, a^2, \ldots, a^d = 1$ різні. Покажемо, що елементи, порядок яких d, – це всі ті $\varphi(d)$ значень a^j, для яких НСД(j, d)=1. По-перше, так як всі d різних степенів різні, то вони є множиною всіх коренів рівняння $x^d = 1$. Отже, довільний елемент,

порядок якого дорівнює d, повинен знаходитися серед степенів елемента a. Але не кожний степінь a має порядок d, оскільки коли НСД$(j,d) = d' > 1$, то елемент a^j матиме менший порядок: числа d/d' і j/d' цілі і тому $(a^j)^{d/d'} = (a^d)^{j/d'} = 1$. Навпаки, покажемо, що елемент a^j при НСД(j,d)=1, має порядок d. Дійсно, припустимо, що НСД(j,d) =1 і a^j має порядок $d'' < d$. Тоді $(a^{d''})^j = (a^{d''})^d = 1$ і, отже, $(a^{d''})^{\text{НСД}(j,d)} = a^{d''} = 1$. Але $a^{d''} \neq 1$, оскільки елемент a має порядок d. Таким чином, a^j має порядок d тоді і тільки тоді, коли НСД(j,d) =1.

Це означає, що коли маємо елемент, порядок якого d, то існує тільки $\varphi(d)$ елементів, порядок яких дорівнює d. Отже, для довільного $d|(q-1)$ існує лише дві можливості: або елементів порядку d немає, або таких елементів $\varphi(d)$.

Але кожний елемент має деякий порядок $d|(q-1)$ і або 0 або $\varphi(d)$ елементів мають порядок d. На підставі тотожності Гауса дістаємо $\varphi(q-1) = \sum\limits_{d|(q-1)} \varphi(d) = q-1$ і права частина дорівнює кількості елементів в F_q^*. Звідси і з того, що кожний елемент має певний порядок, випливає, що для кожного $d|(q-1)$ завжди знайдеться $\varphi(d)$ (і ніколи не 0) елементів, порядок яких дорівнює d. Зокрема, існує точно $\varphi(q-1)$ елементів, порядок яких $q-1$. Як встановлено вище, якщо елемент g має порядок $q-1$, то всі інші елементи порядку $q-1$ – це елементи g^j, для яких НСД$(j,d) = 1$. ■

Наслідок 9. *Для довільного простого числа p існує таке число g, що його степені пробігають всі ненульові класи лишків за модулем p.*

Приклад 2.9.8. Нехай $p = 19$, тоді $p-1 = 18$ і всі лишки за модулем 19 степенів числа 2 породжують всі елементи мультиплікативної групи F_p^*:

2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10,1.

Степені числа $4 = 2^2$ не породжуватимуть всі елементи групи F_p^*, оскільки НСД(2,18)= $= 2 \neq 1$. Дійсно, маємо: 4,16,7,9,17,11,6,5,1,4,16,7,9,17,11,6,5,1. Як бачимо, серед породжених степенями 4 елементів немає, наприклад, 2, 3, 8, 12. ♠

2.9.7 Застосування полів в криптографії

Розглянемо приклад одночасного застосування методів теорії груп і полів в побудові криптографічної системи. Таке застосування, як і у випадку кілець, пов'язане з використанням двох таблиць

– таблиці додавання і таблиці множення елементів поля. Ці таблиці дозволяють, подібно до того як це робилося в кільцях, використовувати гомофонічні шифри.

Нехай, як і раніше, літери алфавіту $X = \{a, b, c, d, \ldots, x, y, z\}$ англійської мови лінійно упорядковані таким чином:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	-
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Додамо до 26 літер англійського алфавіту 27-й символ "-" і побудуємо поле F_{3^3} за допомогою незвідного полінома $f(x) = x^3 + 2x^2 + 1$, що дає такі таблиці додавання і множення. Варто зауважити, що різні незвідні поліноми над одним і тим самим полем лишків даватимуть різні поля.

Адитивна група поля F_{3^3}:

$\oplus$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21	25	26	24
2	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16	20	18	19	23	21	22	26	24	25
3	3	4	5	6	7	8	0	1	2	12	13	14	15	16	17	9	10	11	21	22	23	24	25	26	18	19	20
4	4	5	3	7	8	6	1	2	0	13	14	12	16	17	15	10	11	19	22	23	21	25	26	24	19	20	18
5	5	3	4	8	6	7	2	0	1	14	12	13	17	15	16	11	9	10	23	21	22	26	24	25	20	18	19
6	6	7	8	0	1	2	3	4	5	15	16	17	9	10	11	12	13	14	24	25	26	18	19	20	21	22	23
7	7	8	6	1	2	0	4	5	3	16	17	15	10	11	9	13	14	12	25	26	24	19	20	18	22	23	21
8	8	6	7	2	0	1	5	3	4	17	15	16	11	9	10	14	12	13	26	24	25	20	18	19	23	21	22
9	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8
10	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21	25	26	24	1	2	0	4	5	3	7	8	6
11	11	9	10	14	12	13	17	15	16	20	18	19	23	21	22	26	24	25	22	0	1	5	3	4	8	6	7
12	12	13	14	15	16	17	9	10	11	21	22	23	24	25	26	18	19	20	3	4	5	6	7	8	0	1	2
13	13	14	12	16	17	15	10	11	9	22	23	21	25	26	24	19	20	18	4	5	3	7	8	6	1	2	0
14	14	12	13	17	15	16	11	9	10	23	21	22	26	24	25	20	18	19	5	3	4	8	6	7	2	0	1
15	15	16	17	9	10	11	12	13	14	24	25	26	18	19	20	21	22	23	6	7	8	0	1	2	3	4	5
16	16	17	15	10	11	9	13	14	12	25	26	24	19	20	18	22	23	21	7	8	6	1	2	0	4	5	3
17	17	15	16	11	9	10	14	12	13	26	24	25	20	18	19	23	21	22	8	6	7	2	0	1	5	3	4
18	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	18	22	23	21	25	26	24	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15
20	20	18	19	23	21	22	26	24	25	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16
21	21	22	23	24	25	26	18	19	20	3	4	5	6	7	8	0	1	2	12	13	14	15	16	17	9	10	11
22	22	23	21	25	26	24	19	20	18	4	5	3	7	8	6	1	2	0	13	14	12	16	17	15	10	11	9
23	23	21	22	26	24	25	20	18	19	5	3	4	8	6	7	2	0	1	14	12	13	17	15	16	11	9	10
24	24	25	26	18	19	20	21	22	23	6	7	8	0	1	2	3	4	5	15	16	17	9	10	11	12	13	14
25	25	26	24	19	20	18	22	23	21	7	8	6	1	0	2	4	5	3	16	17	15	10	11	9	13	14	12
26	26	24	25	20	18	19	23	21	22	8	6	7	2	0	1	5	3	4	17	15	16	11	9	10	14	12	13

Остачі від ділення на $f(x)$ позначені такими числами: x – числом 3, $x+1$ – числом 4, $x+2$ – числом 5, $2x$ – числом 6, $2x+1$ – числом 7, $2x+2$ – числом 8, x^2 – числом 9, x^2+1 – числом 10, x^2+2 – числом 11, x^2+x – числом 12, x^2+x+1 – числом 13, x^2+x+2 – числом 14, x^2+2x – числом 15, x^2x+1 – числом 16, x^+2x+2 – числом 17, $2x^2$ – числом 18, $2x^2+1$ – числом 19, $2x^2+2$ – числом 20, $2x^2+x$ – числом 21, $2x^2+x+1$ – числом 22, $2x^2+x+2$ – числом 23, $2x^2+2x$ – числом 24, $2x^2+2x+1$ – числом 25, $2x^2+2x+2$ – числом 26.

Мультплікативна група поля F_{33}:

⊙	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
2	0	2	1	6	8	7	3	5	4	18	20	19	24	26	25	21	23	22	9	11	10	15	17	16	12	14	13
3	0	3	6	9	12	15	18	21	24	11	14	17	20	23	26	2	5	8	19	22	25	1	4	7	10	13	16
4	0	4	8	12	16	11	24	19	23	20	21	25	5	6	1	17	9	13	10	14	15	22	26	18	7	2	3
5	0	5	7	15	11	13	21	26	19	2	4	6	17	10	12	23	25	18	1	3	8	16	9	14	22	24	20
6	0	6	3	18	24	21	9	15	12	19	25	22	10	16	13	1	7	4	11	17	14	2	8	5	20	26	23
7	0	7	5	21	19	26	15	13	11	1	8	3	22	20	24	16	14	9	2	6	4	23	18	25	17	12	10
8	0	8	4	24	23	19	12	11	16	10	15	14	7	3	2	22	18	26	20	25	21	17	13	9	5	1	6
9	0	9	18	11	20	2	19	1	10	17	26	8	25	7	16	6	15	24	22	4	13	3	12	21	14	23	5
10	0	10	20	14	21	4	25	8	15	26	6	16	1	11	18	12	22	5	13	23	3	24	7	17	2	9	19
11	0	11	19	17	25	6	22	3	14	8	16	24	13	21	5	18	2	10	4	12	23	9	20	1	26	7	15
12	0	12	24	20	5	17	10	22	7	25	1	13	15	18	3	8	11	23	14	26	2	4	16	19	21	6	9
13	0	13	26	23	6	10	16	20	3	7	11	21	18	4	17	14	24	1	5	15	19	25	2	12	9	22	8
14	0	14	25	26	1	12	13	24	2	16	18	5	3	17	19	20	4	15	23	7	9	10	21	8	6	11	22
15	0	15	21	2	17	23	1	16	22	6	12	18	8	14	20	7	13	19	3	9	24	5	11	26	4	10	25
16	0	16	23	5	9	25	7	14	18	15	22	2	11	24	4	13	20	6	21	1	17	26	3	10	19	8	12
17	0	17	22	8	13	18	4	9	26	24	5	10	23	1	15	19	6	14	12	20	7	11	25	3	16	21	2
18	0	18	9	19	10	1	11	2	20	22	13	4	14	5	23	3	21	12	17	8	26	6	24	15	25	16	7
19	0	19	11	22	14	3	17	6	25	4	23	12	26	15	7	9	1	20	8	24	16	18	10	2	13	5	21
20	0	20	10	25	15	8	14	4	21	13	3	23	2	19	9	24	17	7	26	16	6	12	5	22	1	18	11
21	0	21	15	1	22	16	2	23	17	3	24	9	4	25	10	5	26	11	6	18	12	7	19	13	8	20	14
22	0	22	17	4	26	9	8	18	13	12	7	20	16	2	21	11	3	25	24	10	5	19	14	6	23	15	1
23	0	23	16	7	18	14	5	25	9	21	17	1	19	12	8	26	10	3	15	2	22	13	6	20	11	4	24
24	0	24	12	10	7	22	20	17	5	14	2	26	21	9	6	4	19	16	25	13	1	8	23	11	15	3	18
25	0	25	14	13	2	24	26	12	1	23	9	7	6	22	11	10	8	21	16	5	18	20	15	4	3	19	17
26	0	26	13	16	3	20	23	10	6	5	19	15	9	8	22	25	12	2	7	21	11	14	1	24	18	17	4

Приклад 2.9.9. Зашифруємо текст з ключовим словом "welcome":
"meeting in twelve".
Користуючись таблицями поля F_{33} дістаємо таку шифрограму:

w	e	l	c	o	m	e	w	e	l	c	o	m	e	w	e	l
m	e	e	t	i	n	g	-	i	n	-	t	w	e	l	v	e
22	4	11	2	14	12	4	22	4	11	2	14	12	4	22	4	11
12	4	4	19	8	13	6	26	8	13	26	19	22	4	11	21	4
7	8	12	18	10	25	1	9	0	21	25	3	7	8	3	25	12
h	i	m	s	k	z	b	k	a	v	z	d	h	i	d	z	m

Дешифрація відбувається таким чином: виписуємо цифри, які відповідають ключовому слову і цифри шифрограми, тобто

w	e	l	c	o	m	e	w	e	l	c	o	m	e	w	e	l
22	4	11	2	14	12	4	22	4	11	2	14	12	4	22	4	11
7	8	12	18	10	25	1	9	0	21	25	3	7	8	3	25	12
12	4	4	19	8	13	6	26	8	13	26	19	22	4	11	21	4
m	e	e	t	i	n	g	-	i	n	-	t	w	e	l	v	e

В рядку таблиці додавання, який відповідає значенню 22, знаходимо значення 7. Тоді у верхньому рядку таблиці знаходимо стовпчик, в якому знайдено значення 7. Це буде номер першої літери тексту явного (в даному випадку це буде число 12, якому відповідає літера m). Продовжуючи діяти таким чином, знаходимо явний текст.

Зашифрувати цей текст можна користуючись таблицею множення:

w	e	l	c	o	m	e	w	e	l	c	o	m	e	w	e	l
m	e	e	t	i	n	g	-	i	n	-	t	w	e	l	v	e
22	4	11	2	14	12	4	23	4	11	2	14	12	4	23	4	11
12	4	4	19	8	13	6	26	8	13	26	19	22	4	11	21	4
16	16	25	11	2	18	24	24	23	21	13	7	16	16	1	22	25
q	q	z	l	c	s	y	y	x	v	n	h	q	q	b	w	z

Одержані шифрограми можна зашифрувати шифром Цезаря або іншим шифром, який використовує властивості підстановок.

Простір ключів для цього поля складає кількість його автоморфізмів. А це число дорівнює кількості способів упорядкування 27-елементої множини, тобто $27! = 10888864450418352160768000000$ способів. Але основною перевагою поля є те, що його мультиплікативна група циклічна і має максимальний порядок.