Из курса «Математики» хорошо известны поля вещественных и комплексных чисел. Эти поля имеют бесконечное число элементов. Поля, из которых строятся коды, имеют ограниченное число элементов.

Ограниченное поле с q элементами называют полем Галуа и обозначают $GF(q)$**.** Операции сложения и умножения осуществляются по модулю q

$(\mathrm{mod}\, q)$.

Пример 1. $GF(2)$

$+$	0	1
0	0	1
1	1	0
$\bullet$	0	1
0	0	0
1	0	1

Пример 2. $GF(5)$**.**

$+$	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

$\bullet$	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

Если $q = p^m$, где p, m - целые положительные числа, то поле $GF(p)$ можно расширить до $GF(p^m)$. Операции сложения и умножения проводятся по модулю $p, (\mathrm{mod}\, p)$.

Пусть C_i и C_j - два кодовых слова в (n,k) кодовом блоке. Мера разницы между C_i, C_j - число позиций, в которых они различаются. Эта мера называется **расстоянием Хемминга** и обозначается $d_{i,j}$, причем $0 < d_{i,j} \le n$, $i \ne j$. Минимальное кодовое расстояние определяется следующим образом: