2MMC10 Cryptology – Fall 2015

September 8, 2015

Finite Fields

Definition (field)**.** A set K is a *field* with respect to $\circ$ and $\diamond$, denoted $(K, \circ, \diamond)$, if

i) $(K, \circ)$ is an abelian group,

ii) $(K^*, \diamond)$ is and abelian group, where $K^* = K \setminus \{e_\circ\}$, and

iii) the distributive law holds in K, i.e.,
$a \diamond (b \circ c) = a \diamond b \circ a \diamond c$ for all $a, b, c \in K$

In other words, a field is a *commutative ring with unity* in which each nonzero element is invertible. In particular there are no zero divisors, i.e., there are no $a, b \neq e_\circ$ such that $a \diamond b = e_\circ$.

Example (field)**.**

- $(\mathbb{Q}, +, \cdot)$ inverse w.r.t. multiplication of $\frac{a}{b}$ is $\frac{b}{a}$ for $a \neq 0$,
- $(\mathbb{C}, +, \cdot)$,
- $(\mathbb{R}, +, \cdot)$,
- $(\mathbb{Z}, +, \cdot)$ is **NOT** a field but a commutative ring with unity, the only invertible elements are $+1$ and -1,
- $(\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}, +, \cdot)$ is a field with $+$ and $\cdot$ defined as in $\mathbb{C}$.

Is there an example for a finite field?

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$\circ$	$e_\circ$	$e_\diamond$
$e_\circ$	$e_\circ$	$e_\diamond$
$e_\diamond$	$e_\diamond$	$e_\circ$

$\diamond$	$e_\circ$	$e_\diamond$
$e_\circ$	$e_\circ$	$e_\circ$
$e_\diamond$	$e_\circ$	$e_\diamond$

$\rightarrow$ XOR and AND...

Definition (subfield)**.** If $(K, \circ, \diamond)$ and $(L, \circ, \diamond)$ are fields and $K \subseteq L$ then K is a *subfield* of L.
$\Rightarrow$ We can add elements of L to and multiply them with elements of K.
$\Rightarrow$ L is a vectorspace over K (other properties work because of the distributive laws).

Definition (extension degree)**.** Let L be a field and let K be a subfield of L. The *extension degree* $[L : K]$ is defined as $\dim_K L$, the dimension of L as a K vectorspace.

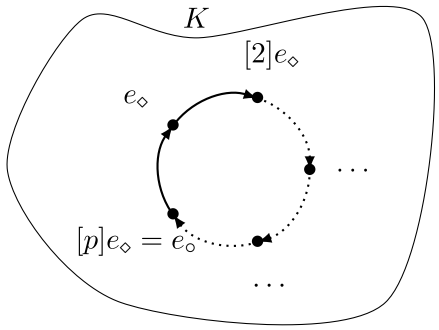
Definition (characteristic)**.** Let K be a field. The *characteristic* of K, denoted $\mathrm{char}(K)$, is the smallest positive integer m such that $\underbrace{e_\diamond \circ e_\diamond \circ \cdots \circ e_\diamond}_{\substack{m \text{ copies of } e_\diamond, \\ \text{denoted as } [m]e_\diamond}} = e_\circ$; if no such integer exists, $\mathrm{char}(K) = 0$.

Lemma. *The characteristic of a field is* 0 *or prime.*

Proof. Let $\mathrm{char}(K) = n = a \cdot b$ with $1 < a, b < n$. Then $e_\circ = [ab]e_\diamond = [a]e_\diamond \diamond [b]e_\diamond$ (repeated application of the distributive law). Since a field has no zero divisors it must be that $[a]e_\diamond = e_\circ$ or $[b]e_\diamond = e_\circ$. $\lightning$ to minimality. $\square$

Lemma. *A finite field K has characteristic p for some prime p.*

Proof. Since K is finite, there must be $i, j \in \mathbb{N}$ with $[i]e_\diamond = [j]e_\diamond$. Let $i > j$, then $[i - j]e_\diamond = e_\circ$ and so $\mathrm{char}(K) | (i - j)$. $\square$



Let K be a finite field. We will now explore its structure. We know already: $\mathrm{char}(K) = p$ for a prime p, and there exists $e_\circ, e_\diamond \in K$ with $e_\circ \neq e_\diamond$. Since K is closed under $\circ$ we do also find $[2]e_\diamond$, $[3]e_\diamond$, $\dots$ $[p-1]e_\diamond$, $[p]e_\diamond = e_\circ$, $[p+1]e_\diamond = e_\diamond$, $\dots$ a cyclic subgroup of order p of $(K, \circ)$. Multiplying two such elements $[i]e_\diamond \diamond [j]e_\diamond = [ij]e_\diamond$ again gives us an element of the set $\{[i]e_\diamond \mid 0 \leq i < p\}$. The scalars are considered modulo p because $[p]e_\diamond = e_\circ$. Since p is prime, $i \cdot j \not\equiv 0 \mod p$ for $0 < i, j < p$. This means that $\{[i]e_\diamond \mid 0 < i < p\}$ forms a subgroup of K^* (the multiplicative group in K; $K^* = K \setminus \{e_\circ\}$). If two structures (groups, rings, fields, …) behave exactly the same way so that one can give a one-to-one map between them, mathematicians call these two structures *isomorphic*. Out considerations have found a subfield of K which is isomorphic to $\mathbb{Z}/_{p\mathbb{Z}}$ with map $[i]e_\diamond \longmapsto i + p\mathbb{Z}$.

Definition (prime field)**.** Let K be a field. The smallest subfield contained in K is called the *prime field* of K.

Lemma. *Let K be a finite field of characteristic p. The prime field of K is isomorphic to $\mathbb{Z}/_{p\mathbb{Z}}$.*

Above we found that an extension field can be considered as a vectorspace over its subfield. From now on we identify the prime field of a finite field with $\mathbb{Z}/_{p\mathbb{Z}}$ and write 0 for $e_\circ$ and 1 for $e_\diamond$. Let $[K : \mathbb{Z}/_{p\mathbb{Z}}] = n$, i.e., the dimension of K as a vectorspace over $\mathbb{Z}/_{p\mathbb{Z}}$ is n. This means that there exists a basis of n linearly independent "vectors" $\alpha_1, \alpha_2, \dots, \alpha_n$ (vectors: elements of L; linearly independent: using coefficients from $\mathbb{Z}/_{p\mathbb{Z}}$ only); this being a basis means that every element in K can be written in a unique way as $\sum_{i=1}^n c_i\alpha_i$ with $c_i \in \mathbb{Z}/_{p\mathbb{Z}}$; the p^n different choices for $(c_1, c_2, \dots, c_n) \in (\mathbb{Z}/_{p\mathbb{Z}})^n$ mean that K has p^n elements.

Lemma. *Let K be a finite field. There exists a prime p and an integer $n \in \mathbb{N}_{>0}$ such that $|K| = p^n$ and $\mathrm{char}(K) = p$. The notation of a field of characteristic p and dimension n is $\mathbb{F}_{p^n}$ or $\mathrm{GF}(p^n)$ (for "Galois field").*

This implies that every finite field has a prime power as its cardinality, so in particular there are no fields of size 6, 10, 14, 15 etc.
In this representation it is very easy to add elements:

$$\left(\sum_{i=1}^n c_i\alpha_i\right) + \left(\sum_{i=1}^n d_i\alpha_i\right) = \sum_{i=1}^n (c_i + d_i)\alpha_i;$$

but for multiplying them we need to know $\alpha_i \cdot \alpha_j$ for $1 \leq i, j \leq n$.
From now on we write $+$ for the first operation $\circ$ and $\cdot$ for the second operation $\diamond$ since we see K as an extension of $\mathbb{Z}/_{p\mathbb{Z}}$.
Let's see whether we can find out more about the multiplicative structure. Rember that for a group G we have $[|G|]a = e$ for any $a \in G$ by the properties of the order of a group. Since K is a field, K^* is a group and it has one element, namely 0, less than K; thus $|K^*| = p^n - 1$.
Recall: The order of an element a in a group G is the least positive integer n such that $a^n = e$. If such an element exists, we know that K^* is cyclic and generated by this element. Observe first that if a has order k and b has order l than $a \cdot b$ has order $\mathrm{lcm}(k, l)$; this construction creates elements of potentially larger order. Remember also that the order of every element divides the group order. Assume that there exists an exponent $e \leq p^n - 1$ such that $a^e = 1$ for all $a \in K^*$. This means that the equation $x^e - 1$ has a root at every $a \in K^*$ — but a non-zero polynomial cannot have more roots than its degree, so $e \geq p^n - 1$. Together this implies:

Lemma. *Let K be a finite field. The multiplicative group K^* is cyclic: $a^{p^n-1} = 1$ for all $a \in K^*$.*

$+$	0	1	a	$a+1$
0	0	1	a	$a+1$
1	1	0	$a+1$	a
a	a	$a+1$	0	1
$a+1$	$a+1$	a	1	0

Are there actually any fields beyond $\mathbb{Z}/_{p\mathbb{Z}}$? We know that they must have p^n elements for some p and n — so what about a field with $2^2 = 4$ elements? This should have a basis of size 2, use $\alpha_1 = 1$ and $\alpha_2 = a$ then $\mathbb{F}_4 = \{0, 1, a, a+1\}$ and we can simply write out the addition table using the vectorspace structure. To write the multiplication table — if possible — we need to know what a^2 is in terms of 1, a, and $a+1$. A table of a group has each element exactly once per row and column. So defining $a^2 = a$ conflict with having already entry a in the first entry of this row. Using $a^2 = 1$ means that $a \cdot (a+1) = a^2 + a = 1 + a$ — but then the third column has already $a+1$ in the first entry. Try $a^2 = a+1$ then $a \cdot (a+1) = a^2 + a = (a+1) + a = 1$ and $(a+1) \cdot (a+1) = a^2 + a + a + 1 = a^2 + 1 = (a+1) + 1 = a$.

$\cdot$	1	a	$a+1$
1	1	a	$a+1$
a	a	a	
$a+1$	$a+1$		

$\cdot$	1	a	$a+1$
1	1	a	$a+1$
a	a	1	$a+1$
$a+1$	$a+1$		

$\cdot$	1	a	$a+1$
1	1	a	$a+1$
a	a	$a+1$	1
$a+1$	$a+1$	1	a

The tables show all group properties except for associativity. We could prove this by checking all combinations but that is very cumbersome.

Let's try another field $\mathbb{F}_8$ with $8 = 2^3$ elements, thus a basis $\alpha_1 = 1$, $\alpha_2 = a$, $\alpha_3 = b$. If we use $a^2 = 1$, we run into the same problems as before; choosing $a^2 = a+1$ constructs the same field as before — no connection with b. So let's try $a^2 = b$; then $a \cdot (a+1) = a^2 + a = b + a$. Again several options for $a \cdot b$. Obviously one can not choose $a \cdot b = a$, b, or $b + a$. Choosing $a \cdot b = 1$ gives $(a+1)(b+a+1) = a \cdot b + a^2 + a + b + a + 1 = 1 + b + b + 1 = 0$ — which is not possible in a field. Similarly $a \cdot b = a + b + 1$ is excluded by $(a+1) \cdot (b+1) = a \cdot b + a + b + 1 = a + b + 1 + a + b + 1 = 0$. Try $a \cdot b = a + 1$:

- $a \cdot (b+1) = a \cdot b + a = a + 1 + a = 1$;
- $a \cdot (b+a) = a \cdot b + a^2 = (a+1) + b$;
- $a \cdot (b+a+1) = \cdots = a + 1 + b + a = b + 1$;
- $(a+1)^2 = a^2 + 1 = b + 1$;
- $(a+1)b = a \cdot b + b = (a+1) + b$;
- $(a+1)(b+1) = a \cdot b + a + b + 1 = (a+1) + a + b + 1 = b$;
- $(a+1)(b+a) = a \cdot b + a^2 + b + a = (a+1) + b + b + a = 1$;
- $b^2 = a^2 \cdot b = a \cdot (a \cdot b) = a \cdot (a+1) = a^2 + a = b + a$;
- $(b+1)(b+a) = b^2 + ba + b + a = (b+a) + (a+1) + b + a = a + 1$
- ...

$\cdot$	1	a	$a+1$	b	$b+1$	$b+a$	$b+a+1$
1	1	a	$a+1$	b	$b+1$	$b+a$	$b+a+1$
a	a	b	$b+a$	$a+1$	1	$b+a+1$	$b+1$
$a+1$	$a+1$	$b+a$	$b+1$	$a+b+1$	b	1	a
b	b	$a+1$	$a+b+1$	$b+a$	a	$b+1$	1
$b+1$	$b+1$	1	b	a	$b+a+1$	$a+1$	$b+a$
$b+a$	$b+a$	$b+a+1$	1	$b+1$	$a+1$	a	b
$b+a+1$	$b+a+1$	$b+1$	a	1	$b+a$	b	$a+1$

How can we get this "automatically"?
How do we compute $a \cdot b = c$ without a lookup table?