Finite Fields

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

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

ii) $(K^*,\circ)$ is and abelian group, where $K^* = K \setminus \{e_0\}$, and

iii) the distributive law holds in $K$, i.e., $a \circ (b \circ c) = a \circ b \circ a \circ c$ 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 $a,b \neq e_0$ such that $a \circ b = e_0$.

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?

$$
\begin{array}{c|cc}
+ & 0 & 1 \\
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array} \quad \begin{array}{c|cc}
\cdot & 0 & 1 \\
0 & 0 & 0 \\
1 & 1 & 0 \\
\end{array} \quad \begin{array}{c|ccc}
\circ & e_0 & e_0 & e_0 \\
e_0 & e_0 & e_0 & e_0 \\
e_0 & e_0 & e_0 & e_0 \\
\end{array}
$$

$\rightarrow$ XOR and AND...

Definition (subfield). If $(K,\circ,\cdot)$ and $(L,\circ,\cdot)$ 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 char($K$), is the smallest positive integer $m$ such that $e_0 \circ e_0 \circ \cdots \circ e_0 = e_0$; if no such integer exists, char($K$) = 0.

$m$ copies of $e_0$, denoted as $[m]e_0$

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

Proof. Let char($K$) = $n = a \cdot b$ with $1 < a,b < n$. Then $e_0 = [ab]e_0 = [a]e_0 \circ [b]e_0$. Since a filed has no zero divisors it must be that $[a]e_0 = e_0$ or $[b]e_0 = e_0$. $\frac{n}{2}$ to minimality.

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 $i|e_0 = [j]e_0$. Let $i > 0$, then $[i-j]e_0 = e_0$ and so char($K$)|(i - j).

$\square$
Let $K$ be a finite field. We will now explore its structure. We know already: $\text{char}(K) = p$ for a prime $p$, and there exists $e_0, e_0 \in K$ with $e_0 \neq e_0$. Since $K$ is closed under $\circ$ we do also find $[2]e_0, [3]e_0, \ldots, [p - 1]e_0, [p]e_0 = e_0, [p + 1]e_0 = e_0, \ldots$ a cyclic subgroup of order $p$ of $(K, \circ)$. Multiplying two such elements $[i]e_0 \circ [j]e_0 = [ij]e_0$ again gives us an element of the set $\{[i]e_0 \mid 0 \leq i < p\}$. The scalars are considered modulo $p$ because $[p]e_0 = e_0$. Since $p$ is prime, $i \cdot j \not\equiv 0 \mod p$ for $0 < i, j < p$. This means that $\{[i]e_0 \mid 0 < i < p\}$ forms a subgroup of $K^*$ (the multiplicative group in $K$; $K^* = K \setminus \{e_0\}$). 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 $[i]e_0 \mapsto i + p\mathbb{Z}$.

**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 $e_0$ and $1$ for $e_0$. 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” $\alpha_1, \alpha_2, \ldots, \alpha_n$ (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 $(c_1, c_2, \ldots, c_n) \in (\mathbb{Z}/p\mathbb{Z})^n$ 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 $\text{char}(K) = p$. The notation of a field of characteristic $p$ and dimension $n$ is $\mathbb{F}_{p^n}$ or $\text{GF}(p^n)$ (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 $-$ for the second operation $\circ$ since we see $K$ as an extension of $\mathbb{Z}/p\mathbb{Z}$.

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>$a$</th>
<th>$a + 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$a$</td>
<td>$a + 1$</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>$a + 1$</td>
<td>$a$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$a + 1$</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$a + 1$</td>
<td>$a + 1$</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

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 $a^2 = a$ a conflict with having already entry $a$ in the first entry of this row. Using $a^2 = 1$ means that $a \cdot (a + 1) = a^2 + a = 1 + a$ — 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 $(a + 1) \cdot (a + 1) = a^2 + a + a + 1 = a^2 + 1 = (a + 1) + 1 = a$. 

2
Similarly, let’s try another field $\mathbb{F}_8$ with 8 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 cannot 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 $a \cdot b = a + 1$:

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

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>a</th>
<th>a + 1</th>
<th>b</th>
<th>b + 1</th>
<th>b + a</th>
<th>b + a + 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>a</td>
<td>a + 1</td>
<td>b</td>
<td>b + 1</td>
<td>b + a</td>
<td>b + a + 1</td>
</tr>
<tr>
<td>a</td>
<td></td>
<td>b</td>
<td>a + 1</td>
<td>b + a</td>
<td>a + 1</td>
<td>b + a + 1</td>
<td>b + 1</td>
</tr>
<tr>
<td>a + 1</td>
<td></td>
<td>b + a</td>
<td>b + 1</td>
<td>a + b + 1</td>
<td>b</td>
<td>1</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>a + 1</td>
<td>a + b + 1</td>
<td>b + a</td>
<td>a</td>
<td>b + 1</td>
<td>1</td>
</tr>
<tr>
<td>b + 1</td>
<td>b + 1</td>
<td>1</td>
<td>b</td>
<td>a</td>
<td>b + a + 1</td>
<td>a + 1</td>
<td>b + a</td>
</tr>
<tr>
<td>b + a</td>
<td>b + a</td>
<td>b + a + 1</td>
<td>1</td>
<td>b + 1</td>
<td>a + 1</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>b + a + 1</td>
<td>b + a + 1</td>
<td>b + 1</td>
<td>a</td>
<td>1</td>
<td>b + a</td>
<td>b</td>
<td>a + 1</td>
</tr>
</tbody>
</table>

Figure 1: Table for $\mathbb{F}_8$.

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

Polynomial ring over field $K$

$$K[x] = \left\{ \sum_{i=1}^{n} a_i x^i \mid n \in \mathbb{N}, a_i \in K \right\}. \text{ } f \in K[x], \text{ } f = \sum f_i x_i.$$

Let $n$ be the largest integer with $f_n \neq 0$ then $\deg(f) = n$, leading coefficient $\text{LC}(f) = f_n$, leading term $\text{LT}(f) = f_n x^n$.

**Definition** (irreducible). A polynomial $f \in K[x]$ is called irreducible if $\deg(f) \geq 1$ and it cannot be written as a product of polynomials of lower degree over the same field, i.e., if $u(x) / f(x)$ then $u(x) \in K$ or $u(x) = f(x)$.

Otherwise $f$ is reducible. Note that this depends on the field $K$. 
Example.
• \(x^2 - 1 = (x + 1)(x - 1)\) is reducible in \(\mathbb{R}[x]\).
• \(x^4 + 2x + 1 = (x^2 + 1)^2\) in \(\mathbb{R}[x]\) has no roots but is reducible.
• \(x^2 + 1\) is irreducible in \(\mathbb{R}[x]\) but reducible in \(\mathbb{C}[x]\) by \((x - i)(x + i)\).
• \(x^3 + 6x^2 + 4\) is irreducible in \(\mathbb{R}[x]\).

The main choice we made in constructing \(\mathbb{F}_8\) was how to write \(a \cdot b\) in terms of the other elements; \(b = a^2\) and so the question was how to represent \(a \cdot b = a^3\) in terms of 1, \(a\), and \(a^2\). We chose \(a^3 = a + 1\) and then all operations followed by using this equality. This polynomial, \(a^3 + a + 1\) does not factor over \(\mathbb{F}_2\); other choices we considered, e.g., \(a^3 + 1\) do factor and it was exactly by considering these factors, e.g., \((a + 1)\) and \((a^2 + a + 1)\) that we derived contradictions, e.g., \((a + 1) \cdot (a^2 + a + 1) = a^3 + 1 = 0\) (using \(a^3 = 1\)). In the end we worked in \(\mathbb{F}_2[a]/(a^3 + a + 1)\) the polynomial ring over \(\mathbb{F}_2\) modulo the irreducible polynomial \(a^3 + a + 1\).

Example. Compute \(a \cdot (a^2 + a)\) and \((a + 1) \cdot (a^2 + a)\) in \(\mathbb{F}_8\) using the irred. polynomial \(a^3 + a + 1\):

\[
\begin{align*}
  a \cdot (a^2 + a) &= a^3 + a^2 & (a + 1) \cdot (a^2 + a) &= a^3 + a \\
  (a^3 + a^2) / (a^3 + a + 1) &= 1 & (a^3 + a) / (a^3 + a + 1) &= 1 \\
  -(a^3 + a + 1) &\quad a^2 + a + 1 & -(a^3 + a + 1) &\quad 1
\end{align*}
\]

In general, this construction gives a finite field.