Finite Fields

We just try to recall what we learnt about (finite) fields. A *field* is a structure, $(K, +, \cdot)$ with two operations, $(K, +)$ is an Abelian (commutative) group with neutral element 0, $(K \setminus \{0\}, \cdot)$ is also an Abelian group. The former group is called the additive group, the latter the multiplicative group of the field. Besides these, we have the distributive laws, namely $(a+b)\cdot c = a\cdot c + b\cdot c$, and $c\cdot(a+b) = c\cdot a + c\cdot b$. We ofter omit $\cdot$, so ab just means $a\cdot b$. If the multiplicative group is not commutative (but all the other properties hold), then the structure is called a *skewfield*. A field cannot have zero divisors, so $ab = 0$ implies that either $a = 0$ or $b = 0$.

What are the easiest examples? Consider the integers modulo m. When is this structure a field? If m is not a prime, $m = uv$, then this means $uv = 0 \pmod{m}$, so the structure has zero divisors (namely u and v), so it cannot be a field. If $m = p$ is a prime, then $K = (\text{mod} p, +, \cdot)$ is a field. We need that every non-zero element has a multiplicative inverse. For this we consider the mapping α, $x \mapsto ax$ for a fixed a. We wish to find the inverse of $a \neq 0$. The mapping α is bijective, because $ax = ay$ implies $a(x-y) = 0$, and from this $x - y = 0$ follows.

What do we know about the additive and multiplicative group? Take e.g. $p = 7$. Then the additive group is the cyclic group C_7. Consider the order of the elements in the multiplicative group. For 2, we have the elements $2, 2\cdot 2 = 4, 4\cdot 2 = 1$, so the order of 2 is 3. Consider 3, we get the elemnts $3, 9 = 2, 6, 18 = 4, 12 = 5, 15 = 1$, so the order of 3 is 6. In other words, 3 generates the multiplicative group, which is a cyclic group of order 6 (that is C_6).

We learnt in general, that the multiplicative group of the modulo p field is cyclic (in number theory we said: *there is a primitive root modulo* p).

Let us also recall the little theorem of Fermat: for every $a \neq 0$ we have $a^{p-1} = 1$, or for every a we have $a^p - a = 0$.

Are there other finite fields? The answer is given in the next theorem, often called the fundamental theorem of finite fields.

Theorem. *The order (number of elemnts) of a finite field F is a prime-power $q = p^h$, p prime. For every prime-power q there is a unique finite field with q elements. I will denote it by* $\mathrm{GF}(q)$.

Consider the elements $0, 1, 1+1, \ldots$. If n is the additive order of 1, then we get back to 0 after n steps. If a is another (non-zero) element, then the additive order of a is the same n, because of distributivity. Namely, $a \cdot (1 + 1 + \ldots 1) = a + a + \ldots + a$. Both sides contain n terms. This also works the other way round, if $a+a+\ldots+a=0$ with s summands, then $1+1+\ldots+1$ is also 0 after s steps. This also implies that n is a prime, if $n=uv$, then for $a=1+\ldots 1$ (u times) and $b=1+\ldots 1$ (v times) we would have $ab=0$, a contradiction since a field has no zero divisors. Note that the elemnts $0,1,1+1,\ldots,1+\ldots 1$ (in the last element we have $p-1$ summands) form a subfield (isomorphic to the modulo p field discussed above). This subfield (denote it by K) is called the prime field of F. Then F is a vector space over K, because of the nice properties of the fields. If the dimension is h, then the order of F is p^h, since an h-dim. vector space has p^h vectors. The multiplicative group of a finite field with q elements has order $q-1$, hence $x^{q-1}=1$ for every non-zero x, hence $x^q-x=0$ for every x. (This is the analogue of the little theorem of Fermat for finite fields.) This also indicates that for the construction of $\mathrm{GF}(q)$, we need the *splitting field* of x^q-x, that is a field in which the elements are exactly the roots of x^q-x.

The number p is called the *characteristic* of the field. (It says that whenever we add up an element p times, then we get 0. A nice consequence is the so-called *Freshmen's dream*: $(a+b)^p=a^p+b^p$. In a more algebraic way, this shows that the map $x\mapsto x^p$ is an automorphism of F. One can show thatthis map (called the *Frobenius automorphism*) generates all automorphisms of $F=\mathrm{GF}(p^h)$, so $|\operatorname{Aut}(\mathrm{GF}(p^h))|=h$ and all automorphisms are of the form $x\mapsto x^{p^i}$ for some $i=0,\ldots h-1$.

The next theorem summarizes what we know about the structure of the additive and multiplicative group of a finite field.

Theorem. *The additive group of* $\mathrm{GF}(q)$, $q=p^h$ *is an elementary Abelian group, that is* $C_p\times C_p\times\ldots C_p$ *(with h factors). The multiplicative group is cyclic, that is there is a primitive element* g*, whose powers give all the non-zero elements of the field.*

The assertion for the multiplicative group follows from the fact that the equation $x^n=1$ has at most n solutions in F if n divides $q-1$. This follows from the fact that a polynomial of degree n can have at most n roots.

The splitting field is an abstract notion, so we need a construction for finite fields which is more concrete.

We wish to construct $\mathrm{GF}(p^h)$. For the construction we need an irreducible polynomial over $\mathrm{GF}(p)$, which has degree h. The field $\mathrm{GF}(p^h)$ will be the factor ring $\mathrm{GF}(p)[x]/(f(x))$, where $(f(x))$ is the ideal generated by $f(x)$ (it consists of the polynomials which are divisible by $f(x)$). More concretely, the elements are the polynomials of degree less than h, addition is the usual addition of polynomials. To multiply two polynomials, the resulting polynomial can have degree at least h, in this case we divide the resulting polynomial by $f(x)$, and the final result of the multiplication will be the remainder of this division.

As an example construct $\mathrm{GF}(4)$. Wee neead an polynomial of degree 2, which is irred. over $\mathrm{GF}(2)$. This is $f(x)=x^2+x+1$. The elements are: $0,1,x,x+1$. Addition is easy, e.g. $x+(x+1)=1$, etc. If we multiply x and $x+1$, the the result is x^2+x, divide it by x^2+x+1, the remainder is 1, so $x(x+1)=1$.

Another relatively simple case is the construction of $\mathrm{GF}(p^2)$, p an odd prime. Take a quadratic non-residue k modulo p (a non-square in $\mathrm{GF}(p)$). Then the polynomial $f(x) = x^2 - k$ is irreducible over GF(p). Use the previous construction. This can be done also in a way similar to the introduction of complex numbers: elements are pairs (a, b) ($a, b \in$ GF(p); they correspond to the polynomial $a+bx$). Define $(a, b)+(c, d) = (a+c, b+d)$ and $(a, b)\cdot(c, d) = (ac+kbd, ad+bc)$. (In case of the complex numbers $k = -1$.)

It is in general not very easy to find an irreducible polynomial of degre h. We will return to this at the end.

The next theorem shows that there are no proper finite skewfields.

Theorem. *(*Wedderburn*) Every finite skewfield is a field (that is, multiplication is commutative).*

What we will also need is the notion of a (simple) field extension. This is about the situation $K \leq F$ that we saw above. In this case F is a vectro space over K, so $|F|$ is a power of $|K|$. Therefore, we have GF(q) $\leq$ GF(q^m). If $\alpha \in$ GF(q^m), then the *minimal polynomial* of α is the polynomial $m_\alpha(x)$, which has leading coefficient 1, has α as a root, and its degree is minimal. So $m_\alpha(\alpha) = 0$. It is straightforward, that $m_\alpha(x)$ is irreducible. We would like to describe $m_\alpha(x)$. The first observation is the following: if $f(x)$ is a polynomial over GF(q) and $f(\alpha) = 0$, then α^q is also a root of $f(x)$. Indeed, the automorhism $x \mapsto x^q$ fixes each element of GF(q). If we apply it to $f(\alpha)$, then the coefficients remain the same and we have to replace α by α^q. This simply says that $f(\alpha^q) = 0$. If we consider the elements $\alpha, \alpha^q, \ldots \alpha^{q^{s-1}}$, where $\alpha^{q^s} = \alpha$, then $\prod_{i=0}^{s-1}(x - \alpha^{q^i})$ divides $f(x)$. This product is a polynomial defined over GF(q). In particular, the minimal polynomial of α is just

$$\prod_{i=0}^{s-1}(x - \alpha^{q^i}).$$

The elements α^{q^i} are called the (algebraic) *conjugates* of α.

A remark on the number of irreducible polynomials: let us fix q and denote the number of irreducible polynomials of degree d by I_d. Then

$$\sum_{d|n} dI_d = q^n,$$

since every element of GF(q^n) belongs to a (unique!) subfield (of order q^d for some $d|n$). (This is a little bit of cheating, since we use that GF(q) exists but the formula can be proven using other arguments.) From this, using Moebius inversion, we get

$$I_n = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}.$$

So, I_n is roughly q^n/n, which more or less means that whenever we choose a polynomial of degree n at random, then it will be irreducible with probability roughly $1/n$.