$\mathbf{F}$ such that $f(X)$ splits into a product of linear factors (equivalently, has d roots in $\mathbf{K}$, counting multiplicity, where d is its degree) and such that $\mathbf{K}$ is the smallest extension field containing those roots. $\mathbf{K}$ is called the *splitting field* of f. The splitting field is unique *up to isomorphism*, meaning that if we have any other field $\mathbf{K}'$ with the same properties, then there must be a 1-to-1 correspondence $\mathbf{K} \tilde{\to} \mathbf{K}'$ which preserves addition and multiplication. For example, $\mathbf{Q}(\sqrt{2})$ is the splitting field of $f(X) = X^2 - 2$, and to obtain the splitting field of $f(X) = X^3 - 2$ one must adjoin to $\mathbf{Q}$ both $\sqrt[3]{2}$ and $\sqrt{-3}$.

7. If adding the multiplicative identity 1 to itself in $\mathbf{F}$ never gives 0, then we say that $\mathbf{F}$ has *characteristic zero*; in that case $\mathbf{F}$ contains a copy of the field of rational numbers. Otherwise, there is a prime number p such that $1 + 1 + \cdots + 1$ (p times) equals 0, and p is called the *characteristic* of the field F. In that case F contains a copy of the field $\mathbf{Z}/p\mathbf{Z}$ (see Corollary 1 of Proposition I.3.1), which is called its *prime field*.

1 Finite fields

Let $\mathbf{F}_q$ denote a field which has a finite number q of elements in it. Clearly a finite field cannot have characteristic zero; so let p be the characteristic of $\mathbf{F}_q$. Then $\mathbf{F}_q$ contains the prime field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, and so is a vector space — necessarily finite dimensional — over $\mathbf{F}_p$. Let f denote its dimension as an $\mathbf{F}_p$−vector space. Since choosing a basis enables us to set up a 1-to-1 correspondence between the elements of this f-dimensional vector space and the set of all f-tuples of elements in $\mathbf{F}_p$, it follows that there must be p^f elements in $\mathbf{F}_q$. That is, *q is a power of the characteristic p.*

We shall soon see that for every prime power $q = p^f$ there is a field of q elements, and it is unique (up to isomorphism).

But first we investigate the multiplicative *order* of elements in $\mathbf{F}_q^*$, the set of nonzero elements of our finite field. By the "order" of a nonzero element we mean the least positive power which is 1.

Existence of multiplicative generators of finite fields. There are $q - 1$ nonzero elements, and, by the definition of a field, they form an *abelian group* with respect to multiplication. This means that the product of two nonzero elements is nonzero, the associative law and commutative law hold, there is an identity element 1, and any nonzero element has an inverse. It is a general fact about finite groups that the order of any element must divide the number of elements in the group. For the sake of completeness, we give a proof of this in the case of our group $\mathbf{F}_q^*$.

Proposition II.1.1. *The order of any $a \in \mathbf{F}_q^*$ divides $q - 1$.*

First proof. Let d be the smallest power of a which equals 1. (Note that there is a finite power of a that is 1, since the powers of a in the finite set $\mathbf{F}_q^*$ cannot all be distinct, and as soon as $a^i = a^j$ for $j > i$ we have