

October 15, 2005

Let \mathbb{F} be a field and $\mathbb{K} \subset \mathbb{F}$ be a subfield i.e., \mathbb{K} is a field and also a subset of \mathbb{F} . In general, given a field \mathbb{F} , then \mathbb{K} is a subfield of \mathbb{F} if it is a subset containing 0 and 1, closed under addition, multiplication and taking inverses. The last requirement says that if $x \neq 0$ is an element in \mathbb{K} , then the inverse x^{-1} (which we know exists in \mathbb{F}) must be in \mathbb{K} .

A typical example is $\mathbb{F} = \mathbb{C}$ and $\mathbb{K} = \mathbb{R}$. \mathbb{R} is a subfield of \mathbb{C} . Other subfields of \mathbb{C} are for example \mathbb{Q} (the field of rational numbers), $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$.

An example from finite fields: recall the field of 3 elements, $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$, and the field of 9 elements $\mathbb{F}_9 = \{a + bi : a, b \in \mathbb{Z}/\mathbb{Z}_3\}$. Then \mathbb{F}_3 is a subfield of \mathbb{F}_9 .

If \mathbb{K} is a subfield of \mathbb{F} , then naturally \mathbb{F} is a vector space over \mathbb{K} . We regard the elements of \mathbb{F} as vectors, they have the addition from \mathbb{F} . Since $\mathbb{K} \subset \mathbb{F}$, we can multiply the elements of \mathbb{F} by elements of \mathbb{K} . This is the scalar multiplication. It's not always true that \mathbb{F} is finite dimensional over \mathbb{K} .

Example 1. \mathbb{C} is an \mathbb{R} -vector space. It has dimension 2, a basis is $\{1, i\}$. This is nothing else than the usual representation of complex numbers as $z = a + bi$, where a is the real part of z and b is the imaginary part.

Moreover, if V is a complex vector space, then it is a real vector space as well. This is because, if V has scalar multiplication by complex numbers, it has in particular, scalar multiplication by real numbers. If V is finite-dimensional over \mathbb{C} , of dimension n and a basis $\{e_1, \dots, e_n\}$, then V is finite dimensional over \mathbb{R} , of dimension $2n$ and with a basis $\{e_1, \dots, e_n, ie_1, \dots, ie_n\}$. In particular the space \mathbb{C}^n is an n -dimensional complex vector space, but an $2n$ -dimensional real vector space.

Example 2. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}\}$ is a 2-dimensional vector space over \mathbb{Q} , with basis $\{1, \sqrt{2}\}$. Note that, since $\sqrt{2}$ is irrational, 1 and $\sqrt{2}$ are linearly independent over \mathbb{Q} .

Example 3. \mathbb{R} is a vector space over \mathbb{Q} . It is infinite dimensional (this statement is equivalent to the fact that \mathbb{R} is uncountable, while \mathbb{Q} and therefore any finite dimensional vector space over \mathbb{Q} are countable).

Example 4. Let \mathbb{F} be a finite field. Consider the set $S = \{1, 1 + 1, 1 + 1 + 1, \dots, \underbrace{1 + 1 + 1 + \dots + 1}_n, \dots\}$. Since this is a subset of \mathbb{F} , it must be finite. But this means there exists an positive integer n such that $\underbrace{1 + 1 + \dots + 1}_n = 0$. Let n be the smallest integer with this property. It is called the *characteristic* of the field. If no such n exists, in particular \mathbb{F} would be infinite, we say \mathbb{F} has characteristic 0. To simplify notation, we will denote by $k \cdot 1$ the element $\underbrace{1 + 1 + \dots + 1}_k$.

The claim is that for a finite field the characteristic is a prime number. Assume it is not: then there exists n_1, n_2 positive integers such that $n_1 n_2 = n$ and $1 < n_1, n_2 < n$. But then $0 = n \cdot 1 = (n_1 \cdot 1) \cdot (n_2 \cdot 1)$. Since \mathbb{F} is a field, it doesn't have zero divisors, and thus we get a contradiction since both $n_1 \cdot 1$ and $n_2 \cdot 1 \neq 0$ (this is because of the minimality of n).

Now, let us denote by p (a prime number) the characteristic of the finite field \mathbb{F} . The set $\mathbb{K} = \{0, 1 \cdot 1, 2 \cdot 1, \dots, (p-1) \cdot 1\}$ is a subfield of \mathbb{F} . One needs to check this claim, in particular the existence of inverses, but it is completely analogous to the proof that $\mathbb{Z}/p\mathbb{Z}$ is a field, so we will not reproduce it here. But then by the considerations above, \mathbb{F} is a vector space over \mathbb{K} . Since \mathbb{F} is finite to begin with, it has to be a finite dimensional \mathbb{K} -vector space, so it is similar to \mathbb{K}^ℓ for some ℓ .

The consequence is that the number of elements in any finite field is a power of a prime number p (and p is the characteristic of \mathbb{F}).