

Let me start by discussing a few things that are taken for granted by Hasse.

A field extension K/F is just a pair of fields K and F with $F \subseteq K$. Well known examples are \mathbb{C}/\mathbb{R} and \mathbb{R}/\mathbb{Q} .

If K/F is a field extension, then K can be interpreted as a vector space over F . In the example above, \mathbb{C} is an \mathbb{R} -vector space: every element of \mathbb{C} can be written as $z = a + bi$; these ‘vectors’ form an additive group, and they can be multiplied (scalar multiplication) by real numbers. If you write a vector (a, b) instead of $a + bi$, it even looks like the vector spaces you know.

Every vector space has a basis; the number of elements in a basis is called its dimension. The dimension $\dim_F K$ of K as an F -vector space is called the degree of the extension, and is denoted by $[K : F]$. For example, $[\mathbb{C} : \mathbb{R}] = 2$, and $\{1, i\}$ is a basis of \mathbb{C} over \mathbb{R} . Note that $[\mathbb{R} : \mathbb{Q}] = \infty$ (this follows from the fact that finite extensions of \mathbb{Q} are countable).

The basic theorem about degrees is the transitivity in towers: If $L/K/F$ is a tower of fields, then $[L : F] = [L : K][K : F]$; for a proof, multiply the basis vectors of K/F with those of L/K and show that this set is a basis for L/F .

Here’s an example: the field $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ has $K = \mathbb{Q}(\sqrt{3})$ as a subfield. The extension L/K has a basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, and the extension K/\mathbb{Q} has a basis $\{1, \sqrt{3}\}$. A basis for L/\mathbb{Q} is given by $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{3}, \sqrt{3}\sqrt[3]{2}, \sqrt{3}\sqrt[3]{4}\}$.

The next result assumed without proof is the existence of primitive elements: given a finite extension K/F of fields of characteristic 0, there always is a $\theta \in K$ such that $K = F(\theta)$. This means that every element $\alpha \in K$ can be written uniquely in the form $\alpha = a_0 + a_1\theta + a_2\theta^2 + \dots + a_{n-1}\theta^{n-1}$, where $n = [K : F]$.

If $[K : F] = 2$, every element of $K \setminus \{F\}$ is primitive. In the example $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ over \mathbb{Q} above, $\theta = \sqrt[3]{2} + \sqrt{3}$ is primitive. In order to prove this, we have to compute the minimal polynomial of θ and show that it has degree 6. We’ll see how to do this later on.

Field extensions of type $K = F(\sqrt[n]{m})$ are called pure; you get arbitrary finite extensions in the following way: take an irreducible polynomial over $F = \mathbb{Q}$, say $f(X) = X^3 + X + 1$. Factor f over some algebraic closure: $f(X) = (X - \alpha)(X - \alpha')(X - \alpha'')$, and put $K = \mathbb{Q}(\alpha)$. This field consists of expressions $a + b\alpha + c\alpha^2$; adding is done coordinatewise, and multiplication is performed as usual, just reduce the result using the relations $\alpha^3 = -\alpha - 1$ and $\alpha^4 = -\alpha^2 - \alpha$.

Showing that this ring is a field is best done with some algebra. Consider the polynomial ring $R = \mathbb{Q}[X]$ and its ideal $I = (f)$. Then R/I is a ring, whose elements are represented by $a + b\alpha + c\alpha^2$, where $\alpha = X + (f)$. It is known that R/I is a field if and only if I is maximal, which for $\mathbb{Q}[X]$ is equivalent to (f) being irreducible. But this is easily checked.