quadratic extension

Canonical name	QuadraticExtension
Date of creation	2013-03-22 15:42:34
Last modified on	2013-03-22 15:42:34
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	20
Author	CWoo (3771)
Entry type	Definition
Classification	msc 12F05
Classification	msc 12F10
Synonym	2-extension
Related topic	PExtension

Let k be a field and K be its algebraic closure. Suppose that $k \neq K$. A *quadratic extension* E over k is a field $k < E \leq K$ such that $E = k(\alpha)$ for some $\alpha \in K - k$, where $\alpha^2 \in k$.

If $a = \alpha^2$, we often write $E = k(\sqrt{a})$. Every element of E can be written as $r + s\sqrt{a}$, for some $r, s \in k$. This representation is unique and we see that $\{1, \sqrt{a}\}$ is a basis for the vector space E over k. In fact, we have the following

Proposition. If the characteristic of k is not 2, then E is a quadratic extension over k iff $\dim(E) = 2$ (as a vector space) over k.

Proof. One direction is clear from the above discussion. So suppose $\dim(E) = 2$ over k and $\{1, \beta\}$ is a basis for E over k. Then $\beta^2 = r + s\beta$ for some $r, s \in k$. Set $\alpha = \beta - \frac{s}{2}$. Then clearly $\alpha \in E - k$ and $\{1, \alpha\}$ is also a basis for E over k. Furthermore, $\alpha^2 = r + \frac{s^2}{4} \in k$. Thus, $k(\alpha)$ is quadratic extension over k and $[k(\alpha) : k] = 2$. But $k(\alpha)$ is a subfield of E. Then $2 = [E : k] = [E : k(\alpha)][k(\alpha) : k] = 2[E : k(\alpha)]$ implies that $[E : k(\alpha)] = 1$ and $E = k(\alpha)$. $\square$

In the proposition above, the assumption that $\mathrm{Char}(k) \neq 2$ can not be dropped. If fact, quadratic extensions of $\mathbb{Z}_2$ do not exist, for if $\alpha^2 \in \mathbb{Z}_2$, then $\alpha \in \mathbb{Z}_2$.

For the rest of the discussion, we assume that $\mathrm{Char}(k) \neq 2$.

Pick any element $\beta = r+s\sqrt{a}$ in $E-k$. Then $s \neq 0$ and $(\beta-r)^2 = s^2a \in k$. So β is a root of the irreducible polynomial $m(x) = x^2 - 2rx + (r^2 - s^2a)$ in $k[x]$. If we define $\overline{\beta}$ to be $r - s\sqrt{a}$, then $\overline{\beta}$ is the other root of $m(x)$, clearly also in $E - k$. This implies that the minimal polynomial of every element in E has degree at most 2, and splits into linear factors in $E[x]$.

Since $\mathrm{Char}(k) \neq 2$, $\beta \neq \overline{\beta}$ are two distinct roots of $m(x)$. This shows that $k(\sqrt{a})$ is separable over k.

Now, let $f(x)$ be any irreducible polynomial over k which has a root β in E. Then the minimal polynomial $m(x)$ of β in $k[x]$ must divide f. But because f is irreducible, $m = f$. This shows that $k(\sqrt{a})$ is normal over k. Since $k(\sqrt{a})$ is both separable and normal over k, it is a Galois extension over k.

Let ϕ be an automorphism of $E = k(\sqrt{a})$ fixing k. Then $\phi(\sqrt{a})$ is easily seen to be a root of the minimal polynomial of $\sqrt{a}$. As a result, either $\phi = 1$ on E or ϕ is the involution that maps each β to $\overline{\beta}$. We have just proved

Theorem. Suppose $\mathrm{Char}(k) \neq 2$. Any quadratic extension of k is Galois over k, whose Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Remark. A quadratic extension (of a field) is also known in the literature as a 2-*extension*, a special case of a p-extension, when $p = 2$.