Bescovitch's theorem on towers of quadratic extensions

Bill Dubuque

A theorem of Bescovitch asserts that if $\mathbb{Q}$ is the field of rational numbers and $p_1, p_2, \ldots, p_r$ be distinct primes, then $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r})\colon \mathbb{Q}] = 2^r$.

We prove a slightly more general fact, namely:
Let Q be a field with $\operatorname{char} Q \neq 2$ and $L = Q(S)$ be an extension of Q generated by n square roots $S = \{\sqrt{a}, \sqrt{b}, \ldots\}$ of elements $a, b, \ldots \in Q$. If every nonempty subset of S has product $\notin Q$ then each successive adjunction $Q(\sqrt{a}), Q(\sqrt{a}, \sqrt{b}), \ldots$ doubles degree over Q so, in total, $[L\colon Q] = 2^n$. Thus the 2^n subproducts of the product of S are a basis of the extension L/Q. First we need a lemma.

Lemma 1. *Let K b a field with $\operatorname{char} K \neq 2$ and $a, b \in K$ with $\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin K$. Then $[K(\sqrt{a}, \sqrt{b})\colon K] = 4$.*

Proof. Let $L = K(\sqrt{b})$. As $[L\colon K] = 2$ by $\sqrt{b} \notin K$, it suffices to show that $[L(\sqrt{a})\colon L] = 2$. This fails only if $\sqrt{a} \in L = K(\sqrt{b}) \Rightarrow \sqrt{a} = r + s\sqrt{b}$ for $r, s \in K$. But this does not hold, because squaring yields

$$a = r^2 + bs^2 + 2rs\sqrt{b}, \tag{2}$$

which is contrary to the hypotheses as the followings show:

$$\begin{aligned} rs \neq 0 \Rightarrow \sqrt{b} \in K & \quad \text{by solving (2) for } \sqrt{b}, \quad \text{(Note that } 2 \neq 0.) \\ s = 0 \Rightarrow \sqrt{a} \in K & \quad \text{via } \sqrt{a} = r + s\sqrt{b} = r \in K \\ r = 0 \Rightarrow \sqrt{ab} \in K & \quad \text{via } \sqrt{a} = s\sqrt{b}, \quad \text{thus } \sqrt{ab} = sb \end{aligned}$$

□

Theorem 3. *Let Q be a field with $\operatorname{char} Q \neq 2$ and $L = Q(S)$ be an extension of Q generated by n square roots $S = \{\sqrt{a}, \sqrt{b}, \ldots\}$ of elements $a, b, \ldots \in Q$. If every nonempty subset of S has product $\notin Q$ then each successive adjunction $Q(\sqrt{a}), Q(\sqrt{a}, \sqrt{b}), \ldots$ doubles degree over Q so, in total, $[L\colon Q] = 2^n$. Thus the 2^n subproducts of the product of S are a basis of the extension L/Q.*

Proof. We proceed by induction on the tower height n = number of root adjunctions. The Lemma above implies $[1, \sqrt{a}][1, \sqrt{b}] = [1, \sqrt{a}, \sqrt{b}, \sqrt{ab}]$ is a Q-vector space basis of $Q(\sqrt{a}, \sqrt{b})$ if and only if 1 is the only basis element in Q. We must lift this to $n > 2$: $[1, \sqrt{a}][1, \sqrt{b}][1, \sqrt{c}] \cdots$ (2^n elements).

$n = 1$ **:** $L = Q(\sqrt{a})$ so $[L\colon Q] = 2$ since $\sqrt{a} \notin Q$ by hypothesis.

$n > 1$ **:** $L = K(\sqrt{a}, \sqrt{b})K$ of height $n - 2$. By induction hypothesis we have $[K\colon Q] = 2^{n-2}$ so we need only show $[L\colon K] = 4$, since then $[L\colon Q] = [L\colon K][K\colon Q] = 4 \cdot 2^{n-2} = 2^n$. The lemma above shows $[L\colon K] = 4$ if $r = \sqrt{a}, \sqrt{b}, \sqrt{ab}$ for $a, b \notin K$ which holds as an induction on $K(r)$ of height $n - 1$ shows $[K(r)\colon K] = 2 \Rightarrow r \notin K$.

□