ANOTHER ELEMENTARY PROOF OF LÜROTH'S THEOREM

by Michaël Bensimhoun

Jerusalem, 10th May 2004

ABSTRACT

We give here another simple proof of Lüroth's theorem. It needs no more than the basics of field theory and Gauss's lemma on primitive polynomials.

Theorem (Luroth): *Let K be a field and M be an intermediate field between K and $K(X)$, for some indeterminate X. Then there exists a rational function $f(X) \in K(X)$ such that $M = K(f(X))$. In other words, every intermediate extension between K and $K(X)$ is simple.*

Proof: We can assume w.l.g. that $M \neq K$ and $M \neq K(X)$. Let $P(Y)$ be the minimal polynomial of X over M,

$$P(Y) = Y^n + r_{n-1}Y^{n-1} + \ldots + r_1 Y + r_0 \quad (r_i \in M \subset K(X)).$$

Necessarily, one the the r_i's, say r_k, does not belong to K, else X would be algebraic over K. For all $i = 0, 1, \ldots, n-1$, let us put $r_i = a_i/b_i$, where $a_i, b_i \in K[X]$, and a_i is coprime to b_i. The polynomial $P(Y)$ can be multiplied by the l.c.m. of the b_i's in order to obtain a primitive polynomial

$$Q(Y) = c_n Y^n + c_{n-1}Y^{n-1} + \ldots + c_0$$

over the ring $K[X]$. Let us consider the polynomials

$$R(X,Y) = a_k(Y)b_k(X) - a_k(X)b_k(Y) \in K[X,Y]$$

and

$$S(Y) = \frac{R(X,Y)}{b_k(X)} = a_k(Y) - \frac{a_k(X)}{b_k(X)}b_k(Y) \in M[Y].$$

Since $R(X,X) = 0$, $Q(Y)$ divides $S(Y)$ in $K(X)[Y]$, therefore it also divides $R(X,Y)$ in $K(X)[Y]$. But $K[X]$ is a unique decomposition domain, hence Gauss's lemma implies that $Q(Y)$ divides $R(X,Y)$ in $K[X,Y]$. Now,

$$\deg_X(R) \leq \max(\deg a_k, \deg b_k) \leq \max(\deg(c_n), \deg(c_k))$$

because

$$\deg(c_n) \geq \deg(b_k) \quad \text{and} \quad \deg(c_k) \geq \deg(a_k).$$

Therefore $\deg_X(R) \leq \deg_X(Q)$. Since Q divides R in $K[X,Y]$, it follows that

$$\deg_X(R) = \deg_X(Q),$$

that is, $R = QT$ where $T \in K[Y]$.

CLAIM: *The polynomial $T(Y)$ is constant: $T(Y) \in K$.*

Proof: Assume, in order to obtain a contradiction, that $\deg(T) > 0$. Put

$$a_k(Y) = q_1(Y)T(Y) + l_1(Y) \quad \text{and} \quad b_k(Y) = q_2(Y)T(Y) + l_2(Y),$$

with $\deg(l_1) < \deg(T)$ and $\deg(l_2) < \deg(T)$. The polynomial $T(Y)$ divides

$$a_k(Y)b_k(X) - a_k(X)b_k(Y),$$

hence also

$$l_1(Y)b_k(X) + l_2(Y)a_k(X).$$

Since $\deg(l_1)$ and $\deg(l_2)$ are less than $\deg(T)$, this is possible only if

$$l_1(Y)b_k(X) + l_2(Y)a_k(X) = 0.$$

But this last equation is impossible since a_k is coprime to b_k, and a_k or b_k is non-constant. Thus, $\deg(T) = 0$ and $T \in K$ as claimed.

From the above claim, it follows that

$$Q(Y) = c\,(a_k(Y)b_k(X) - a_k(X)b_k(Y)), \quad c \in K.$$

Therefore $\deg(P) = \max(\deg(a_k), \deg(b_k))$, or what is the same,

$$[K(X) : M] = \max(\deg(a_k), \deg(b_k)).$$

Furthermore, X is a root of the polynomial $S(Y)$, and $S(Y)$, which belongs to $K(a_k/b_k)[Y] = K(r_k)[Y]$, is of degree equal to $\max(\deg(a_k), \deg(b_k))$; this implies

$$[K(X) : K(r_k)] \leq \max(\deg(a_k), \deg(b_k)).$$

Thus,

$$[K(X) : M] \geq [K(X) : K(r_k)].$$

Finally, since $r_k \in M$,

$$[K(X) : M] = [K(X) : K(r_k)],$$

hence $M = K(r_k)$. ∎